



Brain Computer Interface manufacturers under the data protection lens

A legal analysis of profiling and decision making based on profiling carried out through Brain Computer Interface technology by Emotiv and NeuroSky in the gaming industry

By Ana-Maria Carla Paun

SNR:2065117

**LL.M Law and Technology,
Tilburg Institute for Law, Technology, and Society
Tilburg University Law School
December 2022**

**First supervisor: Dr. Bo Zhao
Second supervisor: Aimen Taimur**

Table of Contents

1.	Introduction	4
1.1.	Background	4
1.2.	Problem statement	5
1.1.	Literature review	6
1.2.	Research question	7
1.3.	Research methods	8
1.4.	Scope and limitations	8
1.5.	Thesis structure	9
2.	Brain Imaging as a door to the mind	10
2.1.	Historical development	10
2.2.	Non-invasive BCIs: fields of applications	11
2.3.	EEG-based BCI games	12
2.3.1.	How does an EEG-based device operate?	13
2.3.2.	Why is EEG technology special?	14
2.4.	Data processing practices	15
2.4.1.	Pre-collection practices	16
2.4.2.	What types of data are collected?	16
2.4.3.	How much data is collected?	17
2.4.4.	Where is the data stored and what are the sharing practices?	18
2.4.5.	How do companies protect data collected through BCI?	19
2.5.	Conclusion	20
3.	GDPR and 20	
3.1.	Introduction	21
3.2.	What is the legal status of brain data under the GDPR?	21
3.2.1.	Defining personal information	23
3.2.2.	Sensitive data	24
3.2.3.	Data processing	26
3.2.4.	Anonymisation: outdated when it comes to neurodata?	26
3.3.	To what extent can current BCI practices be considered compliant to the GDPR?	28
3.3.1.	Lawfulness and transparency	29

3.3.2.	Purpose limitation	31
3.3.3.	Data minimisation, storage limitation and data security	31
3.3.4.	International data transfers	32
3.3.5.	Profiling and profiling based decision making	33
3.5.	Conclusion	36
4.	35	
5.	Appendices	37
	Appendix A.	37
	Emotiv's Privacy Policy	37
	Appendix B.	43
	NeuroSky's Privacy Policy	43
6.	Bibliography	52
	Books	52
	Articles and Papers	53
	Other Online Materials	56
	Opinions	57
	Case Law	57
	Websites	57

1. Introduction

1.1. Background

A few decades ago, the idea of controlling an environment only through thoughts was rendered pure science fiction. However, the advancement in neurotechnology has seen the progressive development of a way to connect individuals to devices: brain computer interfaces (BCIs). The technology represents a historical breakthrough, helping physically impaired patients restore their movement abilities due to variations in brain waves that would be recorded and translated by the machine into a telekinetic action.¹ But as its application expanded beyond the medical sphere and entered the consumer market, concerns arose due to its ability to disseminate an impressive amount and variety of brain information.

High performance Artificial Intelligence (AI) embedded in BCIs are able to decode brain signals in very fine-grained ways, allowing for the unrestricted analysis of emotions, memories, behaviour patterns and intentions of the user not only in a retrospective way, but also in a real-time, rapid and anticipatory manner.² The information yielded does not reveal only trivial facts about the individual, but also has the capacity to disclose information from the most private sphere, going as far as political and religious beliefs, sexual orientation and medical details,³ which could easily be grappled by commercial actors to fulfil their own interests.

Whilst the technology is attractive for the commercial sphere, society is now faced with serious data protection issues.

1.2. Problem statement

The application of non-invasive BCIs based on the electroencephalography (EEG) method has been rapidly adopted in fields like entertainment, games, neuroergonomics, neuromarketing, smart environment, advertising, education, authentication, and security.⁴ But, according to market research, out of all BCI applications, the highest number of users is in the gaming industry.⁵

¹ H.M de Arruda Leite, S.N. Carvalho, T.B Silva Costa et al., ‘Analysis of User Interaction with a Brain-Computer Interface Based on Steady-State Visually Evoked Potentials: Case Study of a Game’, (2018), Computational Intelligence and Neuroscience, available at <<https://doi.org/10.1155/2018/4920132>> accessed 30 May 2021

² S. Rainey, K. McGillivray, S. Akintoye et al., ‘Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?’, (2020), Volume 7, Issue 1, J Law Biosci, available at <DOI: 10.1093/jlb/ljaa051> accessed 21 April 2021.

³ N. Liu, C. Chiang and H. Chin-Chu, ‘Recognizing the Degree of Human Attention Using EEG Signals from Mobile Sensors’, (2013), Volume 13, Issue 8, Sensors, available at <<https://doi.org/10.3390/s130810273>> accessed 25 June 2021.

⁴ S.N. Abdulkader, A. Atia and M.S. Mostafa, ‘Brain computer interfacing: Applications and challenges’, (2015), Volume 16, Issue 2, Egyptian Informatics Journal, 213-230, available at <https://www.sciencedirect.com/science/article/pii/S1110866515000237> accessed 30 May 2021.

⁵ L.F. Nicolas-Alonso and J. Gomez-Gil, ‘Brain Computer Interfaces, a Review’, (2012), Volume 12, Issue 2, Sensors, 1211–1279, available at <doi: 10.3390/s120201211> accessed 30 May 2021.

Giants on the gaming market like Emotiv and NeuroSky have encountered raging success with their wireless EEG devices, Emotiv EPOC headsets (EE headsets) and, respectively, NeuroSky Mindwave Mobile 2 headsets (MWM headsets). The manufacturers have also introduced software development kits and created app stores specifically designed for BCI devices, where developers have unrestricted access to the raw electrical signals that are collected from the players.⁶

But as commercial actors are offered the possibility to peer into the human brain and understand the mental processes of the user, one cannot help but wonder if customers are *adequately* protected from a data protection perspective, especially when these insights are also used for opaque and intrusive processes like profiling and related decision making.

The General Data Protection Regulation (GDPR) is the main piece of legislation concerning data protection in the EU, which provides for a single set of rules across the EU legal framework and addresses these challenges.⁷ It balances the interests of individuals with that of the actors that process personal data, aiming at protecting the freedoms of the former in the digital age.⁸ The Regulation allows for profiling and decision making based on profiling as long as fairness and transparency of the process are ensured, there is a specific legal basis for profiling, data subjects rights are engaged, and, in the last phase, a DPIA is carried out.⁹ The legislation is technologically neutral to prevent creating risk of circumvention, meaning that it does not depend on the emergence of new techniques.¹⁰

But a consumer-grade BCI whose functionality is dependent on the incredible volume and variety of information collected from the human brain appears to threaten the effectiveness of data protection concepts and principles enshrined in the GDPR. Hallinan has already illustrated in her paper a fundamental incompatibility between the activity of BCI and data protection framework, the former raising new challenges due the amount of data collected, its extent and peculiar nature.¹¹ But because profiling and profiling based decision making are very intrusive and opaque practices, it is of the utmost importance that the principles and safeguards enshrined in the GDPR balance the interests of commercial actors with those of the data subjects, despite the challenges raised by this technology.

With gaps in academic literature surrounding profiling and related decision making carried through consumer-grade BCIs in the gaming industry, it must be assessed whether the data protection framework is adequately equipped to protect individuals subjected to these business practices.

This thesis, therefore, aims at assessing to what extent the current level of protection granted to the customers of the EE and MWM headsets under the GDPR is sufficient. It will do so through an analysis of the privacy policies (provided in Appendices A and B) of two renowned

⁶ I. Martinovic, D. Davies, M. Frank, et al., ‘On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces’, (2012), the Proceedings of the 21st USENIX Security Symposium, USENIX, available at <<https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf>> accessed 30 April 2021.

⁷ European Union Agency for Fundamental Rights, Council of Europe, Handbook on European data protection law, (2018).

⁸ *ibid*

⁹ *ibid*

¹⁰ Recital 15 of the GDPR.

¹¹ D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, ‘Neurodata and Neuroprivacy: Data Protection Outdated?’, (2014), Volume 12, Issue 1, Surveillance & Society, available at <<http://journals.sagepub.com/doi/abs/10.1177/002085239606200407?journalCode=rash>> accessed 7 May 2022.

BCI manufacturers in the gaming industry, Emotiv and NeuroSky, considering the peculiar nature of the information collected and the special features of the technology. Special attention will be given to profiling and related decision making, and it will be assessed, based on the legal expertise provided, how invasive these practices are when carried out through BCI technology. Brief recommendations will be provided for commercial actors to improve their corporate policies. Now, there is not enough literature investigating the practices of non-invasive EEG BCIs from a data protection perspective and, in light of the fact that its application in the consumer market is still relatively new and the context is changing rapidly, these recommendations represent only first steps towards better GDPR compliance.

1.3. Literature review

I started the research by looking at scholar articles that provide a general understanding about “Brain Computer Interface”. Once a clear overview of the technology has been provided, I focused on more specific topics such as “legal issues” and “ethical problems”, using academic databases like SSRN, and Google Scholar.

Preliminary findings suggest that when the technology is not assessed from a scientific or commercial point of view, then its ethical aspects are generally the focus of attention. Nevertheless, only a few legal scholars have been identified to address the topic from a privacy side, and even less through a data protection lens.¹² Hence, the current literature is mainly focused on the scientific aspects and the attractiveness of BCI applications for the computer game market, having been referred to as a very promising technology from a commercial perspective and with a great economic potential.¹³

Subsequent research conducted on BCI ethics can be mainly divided between two key areas, psychological effects and physical effects.¹⁴ Burwell et al. is relevant in this sense, having identified common focus points in the literature such as autonomy and identity issues as a consequence of its use, security problems and questions of responsibility, to name just a few.¹⁵ Legal researchers have taken steps in raising awareness about its severe impact on privacy as well, arguing that this technology can easily be turned against the user to infer private information about cognitive processes, adhering to the security of the individual.¹⁶

But only a few legal scholars have come forward with possible suggestions to specifically assess the effectiveness of basic concepts enshrined in the data protection framework. Relevant in this sense is Hallinan et al. that introduces the notion of “neuro data” and renders its uniqueness, raising regulatory and governance questions in the premature phase of the technology.¹⁷ The research article assesses whether the application of the current data protection law is sufficient and adequately equipped for this novelty, illustrating how common

¹² T. Bonaci, D. Hallinan, S. Rainey, and M. Ienca are among the only papers that assess some of the challenges that this technology brings to the data protection framework.

¹³ J.B.F Van Erp, F. Lotte and M. Tangermann, ‘Brain-Computer Interfaces: Beyond Medical Applications’, (2012), Volume 45, Issue 4, Computers, 26-34, available at <DOI:10.1109/MC.2012.107> accessed 30 April 2021.

¹⁴ A. Coin, M. Mulder and V. Dubljev, ‘Ethical Aspects of BCI Technology: What Is the State of the Art?’, (2020), Volume 5, Issue 4, Philosophies, 31-40, available at <<https://doi.org/10.3390/philosophies5040031>> accessed 30 April 2021.

¹⁵ S. Burwell, M. Sample and E. Racine, ‘Ethical aspects of brain computer interfaces: a scoping review’, (2017), Volume 18, Issue 1, BMC Med Ethics, available at <doi:10.1186/s12910-017-0220-y> accessed 21 April 2021.

¹⁶ I. Martinovic, D. Davies, M. Frank, et al., (n. 6).

¹⁷ D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 11).

data protection concepts such as “accuracy” and “sensitive data” are challenged in this context.¹⁸ Bonaci et al. add to the body of research by coming up with solutions to tackle the emerging issues. They suggest the enactment of an interdisciplinary approach of devices, algorithms, and regulations, that aim at enhancing neurosecurity, acknowledging that the current legal framework may be, perhaps, partly outdated by the situation.¹⁹ However, legal scholars do not analyse the challenges brought to the data protection framework by profiling practices and related decision making through BCI technology. Thus, this thesis aims to bridge the gap by analysing these practices carried out through BCI, under the GDPR.

1.4. Research question

Considering the gaps identified in the body of literature, this research paper assesses whether the GDPR is adequately equipped to protect individuals subjected to profiling and profiling-based decision making, or whether this technology provides too many challenges from a data protection perspective, in this context. It aims at doing so by using the privacy policies of the NeuroSky MindWave Mobile 2 (MWM) and Emotiv EPOC (EE) headsets as case study, which are two devices widely spread on the consumer market and have gained rapid popularity. The **central research question** is:

To what extent does the GDPR offer sufficient protection to individuals subjected to profiling and decision making based on profiling through electroencephalography (EEG) by the Mindwave and EPOC headsets?

The research question can be answered by addressing the following **sub-research questions**:

1. *What type of information is collected through BCI technology and to what extent?*
2. *To what extent do the privacy policies of Emotiv and Neurosky reflect their processing practices?*
3. *What is the legal nature of the information collected through BCI?*
4. *How invasive are profiling and decision making based on profiling through BCI under the GDPR?*

1.5. Research methods

To answer the above research question and sub-questions, this thesis will follow a research method based on doctrinal analysis. Because there is no legal framework specifically designed for brain data, this thesis mainly focuses on the analysis of the European Union General Data Protection Regulation (GDPR) as the main piece of legislation, and it also brings into discussion other publications based on their legal authority such as Article 29 Working Party (Art. 29WP) and the European Data Protection Board (EDPB). The paper will use the main legal concepts extracted from the current EU data protection framework that are relevant for this topic, paying special attention to the notions of personal data, sensitive data and profiling.

The four sub-questions that have been identified address the problem from an inward perspective. To evaluate the law in the light of BCI technology, this paper will also apply a

¹⁸ ibid

¹⁹ T. Bonaci, R. Calo and H. Chizeck, ‘App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces’, (2014), IEEE International Symposium on Ethics in Science, Technology and Engineering, Volume 34, Issue 2, 1-7, available at <<https://ieeexplore.ieee.org/document/6893415/>> accessed 30 April 2021.

semi-systematic literature review methodology, using a wide range of technical and scientific articles, and research papers that analyse privacy and security issues.

Understanding the technical features of BCIs is essential to establish how the law should handle it and illustrate its special features, whilst an assessment of the processing practices of Emotiv and NeuroSky will present the facts for the legal analysis following in chapter three. Consequently, these will contribute to answering sub-questions one and two.

In using the research method based on doctrinal analysis, the paper will also assess the legal nature of brain data, explaining its peculiar nature in the GDPR context. Further, to provide an external view, the analysis of NeuroSky's and Emotiv's privacy policies will allow for an assessment of the law in practice. This will help in assessing the tension between the operational framework of the EE and MWM headsets and GDPR's data protection principles and rules. As a result, sub-questions three and four will be answered.

1.6. Scope and limitations

The scope of this thesis is limited to profiling practices and decisions made on its basis through the *NeuroSky Mindwave Mobile 2* and *Emotiv EPOC* EEG headsets, which are responsible for collecting and interpreting the data that is further stored in one of the endpoints.

While there are multiple types of BCIs on the market and which are based on various technologies such as invasive electrocorticography (ECoG) and microelectrode arrays (MEAs), any other type than non-invasive BCIs based on electroencephalography is outside the scope of this thesis. This is because non-invasive EEG BCI is the technology with the most promising marketable future due to its portability, low price, and ease of use.²⁰ Similarly, BCI technology has expanded its application in numerous fields, as previously explained, but this thesis will focus only on its activity in the gaming industry, and, even more specifically, it will assess the privacy policies of two BCI manufacturers, NeuroSky and Emotiv. The reason for focusing on the gaming industry is its popularity among many users, whilst Emotiv and NeuroSky have been selected due to their leading market position.

Solely automated decision making is left out of the scope.²¹ The privacy policies are formulated in a broad and ambiguous manner, especially when it comes to profiling. The practices taking place in the background are largely carried out in an opaque manner, and to be able to assess solely automated decision making, more facts need to be provided by the manufacturers and developers to build the legal analysis. Additionally, while there are further safeguards and conditions imposed for profiling practices,²² this thesis will explore more extensively only the concepts of transparency and fairness, data minimisation, storage limitation, purpose limitation and data security principles, and the rules surrounding international transfers. From a legal perspective, the reason to focus only on these concepts is that, based on the nature of the information extracted through BCIs and its practices, so far these are the most challenged from the data protection framework.

Moreover, whilst the nature of the information extracted from the brain is extensively assessed, especially in the context of the legal framework, it is important to mention that this thesis does

²⁰ S.N. Abdulkader, A. Atia and M.S. Mostafa, (n. 4).

²¹ Article 22(1) of the GDPR.

²² See "Data protection principles" and "Data subject rights" sections in Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, ('WP251'), 2017.

not provide a complete analysis of brain data and its peculiar characteristics, since limited neuroscience expertise has been used.

Finally, the recommendations for commercial actors to improve their corporate policies provided in the last chapter, in addition to the one for better preserving privacy, are important first steps towards better GDPR compliance. However, for now, because of the infancy of the technology and the fast-changing context, they do not claim to be long term solutions, but only short term.

1.7. Thesis structure

Each of the chapters from the thesis will answer different sub-research questions, contributing to answering the overall research question.

The second chapter is facts-based, setting the scene for the legal analysis. It discusses the evolution of brain computer interface technology and its application. In doing so, it illustrates the particularities of this technology, which provide EE and MWM headsets with the potential of becoming a door to the human mind because of the vast volume and variety of information collected. The terms of use of NeuroSky and Emotiv will be assessed, and, based on the insights provided about the technology, it is analysed to what extent their terms of use reflect the reality of their processing practices. This chapter will answer sub-research questions one and two.

The third chapter illustrates the peculiarity and uniqueness of brain data and assesses its legal nature. In light of these, it assesses and compares the privacy policies of NeuroSky and Emotiv, analysing to what extent are challenged fundamental principles and rules enshrined in the data protection framework. These provisions are important safeguards for users of the EE and MWM headsets, which are subjected to profiling and related decision making. Consequently, the chapter will illustrate how invasive these practices are when carried out through BCI technology and answer sub-research questions three and four.

Lastly, the final chapter summarises the findings of the thesis, outlining the main issues from a data protection perspective regarding this new technology. It provides brief recommendations for commercial actors to improve their corporate policies as first steps towards better GDPR compliance.

2. Brain Imaging as a door to the mind

To assess in the third chapter how the GDPR treats BCI technology and whether a need for greater data protection is preferable, it is essential to first understand the development of the technology and how it operates.

This chapter aims to provide the reader with a better understanding of BCI technology, focusing on what type of information it collects and its amount. Devices based on non-invasive EEG BCI technology like the EE and MWM headsets marketed by Emotiv and, respectively, NeuroSky, present certain special features that allow them to disseminate an extraordinary volume of information and are highly intrusive. Taking these characteristics into consideration, the chapter will analyse to what extent the EE and MWM headsets adhere to the processing practices that are detailed by the two companies in their terms of use.

Further through the evolution of intelligence-driven technology, brain computer interface systems have rapidly extended far beyond the clinical sphere.²³ The application in the gaming industry will be the focus of this thesis as a case study because of its popularity among a large number of users, whilst the electroencephalography method will be at the forefront of the discussion due to its advantages for the consumer market. The first part will contextualise the technology, whereas the second part will dive into the terms of use of EE and MWM headsets, scrutinising the practices of Emotiv and NeuroSky.

2.1. Historical development

Based on the method employed to observe brain activity, brain computer interface systems can be classified into two main groups: invasive and non-invasive. The analogy between the two lays in the electrode placement.²⁴ An invasive procedure like electrocorticography (ECoG) sees the individual undergoing surgery to have the electrodes directly implemented into the brain.²⁵ While brain signals are prone to better analysis because the electrodes are placed within the skull, surgically implanted chips carry serious long-term risks of infections and haemorrhages, preventing the method from becoming consumer-grade deployed in the near future. In contrast, during the non-invasive method, electrodes are simply attached to the human scalp through gel and wired to a computer.²⁶ More recently, even this procedure was simplified, with electrodes finding their way into headsets,²⁷ baseball caps,²⁸ or headbands,²⁹ which are connected to the translation unit (i.e a computer) through wireless.³⁰ Although brain waves are to some extent attenuated by the time they reach the translation unit as they have to pass through the dura, skull and scalp in the process, the enhanced wearability and user-safety outweigh its invasive counterpart, successfully entering the consumer market.³¹ The most common non-invasive methods are functional magnetic resonance imaging (fMRI) and electroencephalography (EEG), and, while the latter operates by recording neural activity, the former works by

²³ J. Shih, D. Krusienski and J. Wolpaw, 'Brain-Computer Interfaces in Medicine', (2012), Volume 87, Issue 3, Mayo Clinic Proceedings, 268–279, available at <doi: 10.1016/j.mayocp.2011.12.008> accessed 20 April 2021.

²⁴ P. Chaudhary and R. Agrawal, 'Emerging Threats to Security and Privacy in Brain Computer Interface', (2018), Volume 3, Issue 12, Int. J. of Adv. Studies of Scientific Research, available at <<https://ssrn.com/abstract=3326692>> accessed 8 May 2021.

²⁵ M. Ahn, M. Lee, J. Choi and S.C. Jun, 'A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users', (2014), Volume 14, Issue 8, Sensors, 14601-14633, available at: <doi: 10.3390/s140814601> accessed 20 April 2021.

²⁶ Q. Li, D. Ding and M. Conti, 'Brain-Computer Interface applications: Security and privacy challenges', (2015), IEEE Conference on Communications and Network Security (CNS), 663-666, available at: <http://doi: 10.1109/CNS.2015.7346884> accessed 8 May 2021.

²⁷ J. Xu, R.F. Yazicioglu, B. Grundelner et al., 'A 160uW 8-Channel Active Electrode System for EEG Monitoring', (2011), IEEE Transactions on Biomedical Circuits and Systems, Volume 5, Issue 6, 555-567 available at <doi: 10.1109/TBCAS.2011.2170985> accessed 20 May 2021.

²⁸ T.J. Sullivan, S.R. Deiss et al., 'A Brain-Machine Interface Using Dry-Contact, Low-Noise EEG Sensors', (2008), IEEE International Symposium on Circuits and Systems, 1986-1989, available at <<https://ieeexplore.ieee.org/document/4541835>> accessed 15 May 2021.

²⁹ L. Liao, I. Wang, C. Chang et al., 'Human Cognitive Application by Using Wearable Mobile Brain Computer Interface', (2010), TENCON 2010 - 2010 IEEE Region 10 Conference, 346-351, available at <doi: 10.1109/TENCON.2010.5686646> accessed 15 May 2021.

³⁰ R.F. Rezai., 'Brain-Computer Interface Systems - Recent Progress and Future Prospects', (IntechOpen, 5 June 2013), available at < <https://www.intechopen.com/books/3532>> accessed 20 April 2021.

³¹ M. Akhtari, H.C. Bryant and A.N. Mamelak, 'Conductivities of three-layer human skull', (2002), Volume 14, Issue 3, Brain Topogr, 151-67, available at <doi: 10.1023/a:1014590923185> accessed 30 May 2021.

measuring changes in blood volume, flow and oxygenation.³² The latter will be the focus of this thesis as it is the most popular one due to its portability, ease of use and reduced price, which have prompted its application to spread into multiple fields.³³

2.2. Non-invasive BCIs: fields of applications

During its emergence in the 1960s, the technology was the epicentre of attention due to its capability to help patients left impaired because of neuromuscular disorders. Brain computer systems would restore their movement abilities through telekinetic action carried out by prosthetic devices.³⁴ 60 years later the technology continues to revolutionise other fields, with wireless EEG devices having been successfully adapted to real-life applications.³⁵ In the educational field, Zhang and others have demonstrated that students can learn English better by making use of BCIs.³⁶ EEG-based BCI devices in neuromarketing are described as a ground breaking development research, being deployed to record the highest quality data on consumers.³⁷ In terms of cybersecurity, EEG technology could increase user security by deploying brain signals as a biometric signature for identification and authentication purposes.³⁸ A. Campbell and others have proposed an app that enables the user to dial contacts from the smartphone's address book only by virtue of his brain signals, among other discussed ideas.³⁹ The user is shown a series of photos from the address book and selects the person he wishes to call through an inevitable change in his brain waves triggered when reaching the photo of the desired contact.

Perhaps the most influential application of BCI technology is in the gaming industry, which is also the most illustrative field for privacy-related risks for a number of reasons.⁴⁰ The gaming addiction has become stronger over the past years and it is expected to continue to gain grounds at an even higher rate due to the pandemic, which has forced many to move their life and develop new interests in the virtual space. The industry is known for manipulating and

³² V. Menon and S.C. Herbert, 'Combined EEG and fMRI Studies of Human Brain Function', (2005), Volume 117, Issue 3, *Int Rev Neurobiol.*, 291-321, available at <DOI: 10.1016/S0074-7742(05)66010-2> accessed 21 May 2021.

³³ S.N. Abdulkader, A. Atia and M.S. Mostafa, (n. 4).

³⁴ H.M de Arruda Leite, S.N. Carvalho, T.B Silva Costa et al., (n. 1).

³⁵ A. Krugliak and A. Clarke, 'Towards real-world neuroscience using mobile EEG and augmented reality', (2022), Volume 12, *Sci. Rep.*, available at <<https://doi.org/10.1038/s41598-022-06296-3>> accessed 25 April 2021.

³⁶ L. Zhang, 'A web-based English teaching module on the administration of electroencephalography-based neurofeedback training for Chinese students', (2018), Volume 16, Issue 5, *NeuroQuantology*, 693-698, available at <DOI: 10.14704/nq.2018.16.5.1243> accessed 30 May 2021.

³⁷ G. Vecchiato, L. Astolfi, F. De Vico Fallani, et al., 'The study of brain activity during the observation of commercial advertising by using high resolution EEG techniques', (2009), *Engineering in Medicine and Biology Society, Annual International Conference of the IEEE*, 57-60, available at <<https://www.ncbi.nlm.nih.gov/pubmed/19965113>> accessed 30 May 2021.

³⁸ The authors found a classification accuracy of over 80%. See M. Polous, M. Rangoussi and N. Alexandris, 'Neural network-based person identification using EEG features', (1999), Volume 2, Issue 1, *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1117-1120, available at <doi: 10.1109/ICASSP.1999.759940> accessed 31 May 2021.

³⁹ A. Campbell, T. Choudhury, S. Hu, H. Lu et al., 'Neurophone: brain mobile phone interface using a wireless EEG headset', (2010), *Proceedings of the second ACM SIGCOMM workshop on Networking, Systems, and Applications for Mobile Handhelds, MobiHeld 2010*, 3-8, available at <DOI:10.1145/1851322.1851326> accessed 30 May 2021.

⁴⁰ According to a market research, out of all BCI applications, the highest number of potential users is in the gaming industry. See L.F. Nicolas-Alonso and J. Gomez-Gil, (n. 5).

exploiting the vulnerabilities and cognitive biases of its customers.⁴¹ And, while the main audience of the industry is the youth, the number of gaming adepts within under aged teenagers is increasing at a high speed. Therefore, the focus of this thesis will be on the gaming industry.

2.3. EEG-based BCI games

A handful of companies like MindSolutions, Muse and MyndPlay have encountered a roaring success after the deployment of their consumer grade brain computer interfaces, along with software development kits, BCI app stores and open-source platforms specially set up in order to further facilitate the augmentation of applications.⁴² But this thesis will only focus on NeuroSky, with its MindWave Mobile 2 headsets (referred to as MWM headsets) and Emotiv's Emotiv EPOC headsets (referred to as EE headsets), because of their leading market position.⁴³

High-performance Machine Learning algorithms embedded in both the EE and MWM headsets make predictions based on the patterns discovered in the information collected about their users. This, in turn, enables NeuroSky and Emotiv to comprehend and study large and complex datasets.⁴⁴ BCI technology based on EEG also presents certain particularities provided through the deployment of artificial stimuli that lead to involuntary mental responses, and the employment of mental strategies that trigger multiple and various changes in brain activity.

2.3.1. How does an EEG-based device operate?

In BCI practices it is mostly traditional machine learning (ML) algorithms that are involved.⁴⁵ ML algorithms are known for developing "intelligence" over time due to their ability to train themselves and optimise their application to boost performance.⁴⁶ Moreover, it is most likely that the technology and its ability to extract and interpret data will proportionally evolve along with the digital field.

The following image illustrates the cycle of the EEG signals, from the moment they are captured to when the output is retrieved.

⁴¹ So much so that gaming disorders have been included on the list of mental health conditions. See L. Gros, N. Debye, J. Lete and C. Leemput, 'Video Game Addiction and Emotional States: Possible Confusion Between Pleasure and Happiness?', (2020), *Front. Psychol.*, available at <<https://doi.org/10.3389/fpsyg.2019.02894>> accessed 3 June 2021.

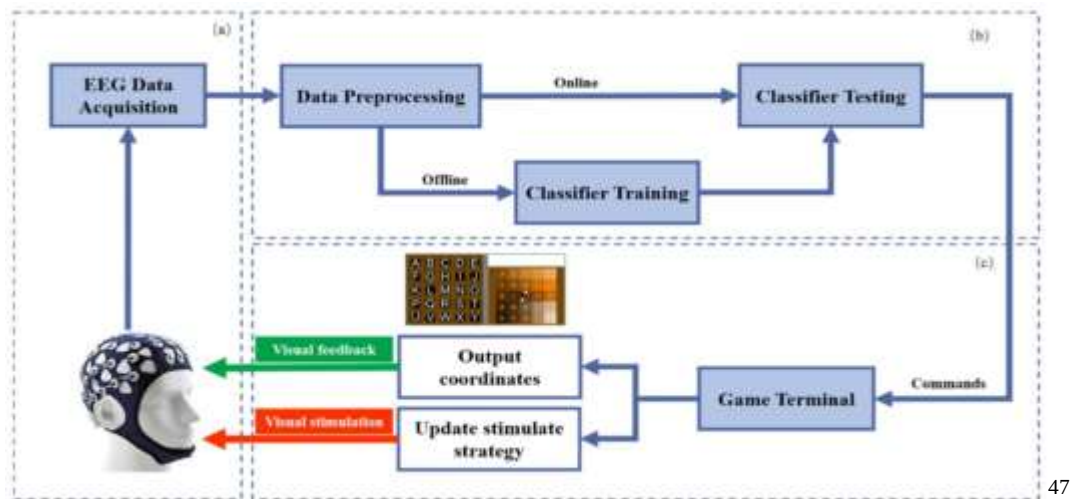
⁴² I. Martinovic, D. Davies, M. Frank, et al., (n. 6).

⁴³ The Global Smart EEG Headset market is expected to develop at a considerable rate between 2022 and 2028, with leading key players being Emotiv and NeuroSky. See <https://southeast.newschannelnebraska.com/story/46355853/eeeg-headset-market-2022-top-companies-report-covers-industry-outlook-in-depth-analysis-business-opportunities-and-market-share-demand-forecast-cagr> accessed 6 September 2022.

⁴⁴ Vijay Kanade, 'Top 10 Machine Learning Algorithms in 2022', (Spiceworks, 30 May 2020), available at <https://www.spiceworks.com/tech/artificial-intelligence/articles/top-ml-algorithms/> accessed 27 April 2021.

⁴⁵ *ibid*

⁴⁶ S. Rainey, K. McGillivray, S. Akintoye et al., (n. 2)



Five phases can be identified in the EEG-based BCI systems used in gaming; (1) acquisition of the neurosignal through the electrodes; (2) pre-processing of these brain signals for reducing noise and removing any other artefacts that may distort their quality (i.e. eye blinking); (3) the important features are extracted, selected and classified (i.e the features that point to stimuli and commands, from which information can be inferred); (4) commands that will be carried out by the application are generated; and, finally, (5) feedback is given to the user about the performance of his mental activity during the game. Although traditional ML algorithms are embedded in BCI devices, with the rapid development that deep learning has seen, novel and more complex computational architectures with higher levels of accuracy have been proposed for the BCI systems.⁴⁸

In addition to its operational power, understanding why this technology is special will also help in the assessment of Emotiv's and NeuroSky's collection processes.

2.3.2. Why is EEG technology special?

Multiple electrical variations in the human brain created by artificial stimuli trigger involuntary mental responses that are unique for every person and that enable the collection of an impressive amount of data.

The EEG is an electrical signal spawned by the cumulative activity of neuronal generators rich in information relating to an individual.⁴⁹ Although known to be susceptible to noise and signal distortion, EEG signals are easily measurable and have a good temporal resolution.⁵⁰ Recorded through sensitive electrodes, these capture 5 types of brain waves (gamma, beta, alpha, theta and delta). Each indicates different emotional states and possible variations like excitement,

⁴⁷ M. Li, F. Li, J. Pan et al., 'The MindGomoku: An Online P300 BCI Game Based on Bayesian Deep Learning', (2021), Volume 21, Issue 5, Sensors, available at <doi: 10.3390/s21051613> accessed 1 June 2021.

⁴⁸ AlexNet and GoogleNet, for example, which have been recently developed, achieved a very high level of accuracy in image classification. See K. Zhang, G. Xu, X. Zheng et al., 'Application of Transfer Learning in EEG Decoding Based on Brain-Computer Interfaces: A Review', (2020), Volume 20, Issue 21, Sensors, available at <<https://doi.org/10.3390/s20216321>> accessed 1 June 2021.

⁴⁹ T. Kirschstein and R. Köhling, 'What is the source of the EEG?', (2009), Volume 40, Issue 3, Clin EEG Neurosci, 146-9, available at <doi: 10.1177/155005940904000305> accessed 20 June 2021.

⁵⁰ Q. Li, D. Ding and M. Conti, (n. 26).

arousal, concentration, eye blinking and other cognitive reactions that typically occur in video game players.⁵¹

EEG signals provide a new opportunity to represent an individual through data. The method enables a higher amount of precision in recording the underlying cognitive activities that are at the very core of any person, enabling the display of more quantitative and qualitative information due to their raw and involuntary collection directly from the brain.⁵² The richest amount of information is collected from the EEG signals when there are multiple and various changes in brain activity.⁵³ For conventional video games, the user presses a button or uses the mouse to convey information to the device. In BCI-games systems, that requirement is replaced by a “control paradigm”, the trigger that determines changes in the power spectra rhythms of the 5 frequencies that are recorded by the machine, and, after their processing and interpretation, they reveal valuable data about their possessor.⁵⁴

The electrical variations are either naturally provoked by the player due to his deep engagement in the game, or manually caused by a third party, to trigger and collect measurable patterns about him.⁵⁵ This is what companies deploying BCI technology do: employing mental strategies like the Event-Related Potential (ERP) and steady-state visual evoked potential (SSVEP) to manually trigger variations in patterns of electrical signals through stimuli.⁵⁶ Emotiv and NeuroSky may have one of the largest capabilities when it comes to stimuli deployment, with the former acknowledging the variety of stimuli that it has at display (see Appendix A, para 2). The use of stimuli can even take place beyond the conscious perception of the individual and remain undetected by being embedded in a standard and consciously recognised one. Stimuli can also be combined rather than used in isolation from one another.⁵⁷ In addition to using the above-mentioned approaches, the machine learning algorithms that govern the stimuli deployment are tasked with improving their quality by continuously tailoring them to every user’s cognitive activity through previous information collected about him. The more the stimulus is related to the user and the stronger his unconscious response is, the bigger the chance to capture sensitive information and high amounts of data, as the response recorded by the BCI is sharper.⁵⁸ These variations in band frequencies reveal diverse and high amounts of information that the user cannot control and may in fact not even be aware of.⁵⁹ For example, studies have shown that a longer P300 latency is found predominantly only in patients that suffer of epilepsy,⁶⁰ information that gaming companies like Emotiv and NeuroSky should not be able to collect.

⁵¹ T. Kirschstein and R. Köhling, (n. 49).

⁵² D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 11).

⁵³ Q. Li, D. Ding and M. Conti, (n. 26).

⁵⁴ M. Ahn, M. Lee, J. Choi and S.C. Jun, (n. 25).

⁵⁵ F. R. Reza, B.Z Allison, C. Guger et al., ‘P300 brain computer interface: current challenges and emerging trends’, (2012), Volume 5, Issue 14, *Frontiers in Neuroengineering*, available at <doi: 10.3389/fneng.2012.00014> accessed 22 June 2021.

⁵⁶ A. Stopczynski, D. Greenwood, L.K. Hansen and A.S. Pentland, ‘Privacy for Personal Neuroinformatics’, (2014), *Computer Science*, available at < DOI:10.2139/SSRN.2427564> accessed 5 May 2021.

⁵⁷ *ibid*

⁵⁸ L.A. Farwell, ‘Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials’, (2012), Volume 6, Issue 2, *Cogn Neurodyn*, 115-154, available at <doi: 10.1007/s11571-012-9192-2> accessed 22 June 2021.

⁵⁹ *ibid*

⁶⁰ Z. Rui, M. Li, Q. Chen et al., ‘The P300 Event-Related Potential Component and Cognitive Impairment in Epilepsy: A Systematic Review and Meta-analysis’, (2019), Volume 10, Issue 1, *Front Neurol*, available at <<https://doi.org/10.3389/fneur.2019.00943>> accessed 23 June 2021.

The features previously illustrated confer a special nature to BCI technology, providing it with the ability to disseminate an extraordinary amount of information, to an in-depth extent. The remainder of the chapter will assess, in light of the special characteristics of BCI and the technological expertise provided so far, whether the terms of use of the EE and MWM headsets mirror how the devices operate and how personal information is actually handled.

2.4. Data processing practices

During this research, strong discrepancies have been found first and foremost between the terms of use explaining how the devices operate, how personal information is used and handled, and the practical reality of the processing practices.

This part will dive into an assessment of Emotiv's and NeuroSky's terms of use, looking at what type of information can be collected from the human brain and how the companies collect, store, share and protect this information, assessing to what extent their terms of use reflect their data processing practices. The reality is that due to the characteristics of BCI and the EEG method, data processed through BCI cannot follow the processing practises detailed in their terms of use.

In demonstrating this, the section will assess: (a) the pre-collection practices; (b) the types of information collected; (c) the quantity of the information; (d) storage and sharing practices; and (e) the standard of protection.

2.4.1. Pre-collection practices

Transparency, simplicity and control of data as detailed by both companies (see Appendices A and B, para 1), is not possible in a BCI environment due to the raw nature of the EEG signals at the time of collection and the Machine Learning techniques employed.

At the collection stage, neurosignals have not been de-coded yet. They are captured in their raw form, representing mere waves deployed on a screen.⁶¹ Because of this, it is unclear at the collection point in time what type of information they contain, rendering it impossible for the companies to be transparent about the information collected.

Customer control over one's personal information is, similarly, unachievable. The information that can be inferred from the neurosignals collected is unknown yet at this stage. Commercial actors want to ensure that they fulfil their interests and collect the information that they need (i.e performance parameters).⁶² Thusly, there is no selective discrimination between the electrical signals that have been recorded, with all the EEG data being sent in bulk to the online platform for pre-processing. It is only during that phase that the raw EEG data is interpreted and translated, displaying all the information that could be inferred from that brain signal.⁶³ Since this is how the technology operates and engaging in the video game is intrinsically conditioned to the collection and interpretation of the raw data, this leaves the customer with no choice but to allow the company to collect the information in full.

⁶¹ E.A Larsen, M.Z Ilyas, M.I Ahmad and A.R.I. Ghani, 'Classification of EEG Signals in a BrainComputer Interface System', (2016), 2016 International Conference on Robotics, Automation and Sciences (ICORAS), 1-4, available at <doi: 10.1109/ICORAS.2016.7872610> accessed 30 June 2021.

⁶² B. King, '10 Manipulative Gaming Tactics You Fall For Every Time', (WhatCulture, 13 September, 2021), available at <https://whatculture.com/gaming/10-manipulative-gaming-tactics-you-fall-for-every-time> accessed 8 September 2022.

⁶³ E. A. Larsen, M.Z Ilyas, M.I Ahmad and A.R.I. Ghani, (n. 61).

As explained, ML algorithms are employed in BCI technology to ensure the quality and quantity of information collected. The operational framework of the BCI is based on complex AI algorithms, rendering it impossible for companies to explain BCI's nature and how it works in clear and simple terms. Since the device is based on deep learning techniques, it uses millions of data points as inputs in order to produce an output.⁶⁴ The method is known for being largely self-directed and generally difficult for data scientists and programmers to interpret, which is one of the characteristics of black box development.⁶⁵ As such, not even manufacturers or controllers understand the logic behind the processing practices, let alone trying to make customers fully comprehend it, along with the risks and consequences.

These poor pre-collection practices enable the Emotiv and NeuroSky to collect in-depth information about their users.

2.4.2. What types of data are collected?

According to research findings, the information collected about users is highly intrusive, and children under the age of 16 also count themselves among their customers.

The variety of the data that can be extracted has been the front debate in many experiments.⁶⁶ To only mention a few, studies have yielded that age and gender can be inferred from recorded EEG signals, the alpha rhythm can reveal a general pattern of the concentration of the user (i.e. how it decreases, different levels and peaks) and studying the power spectra of the theta and alpha bands can determine whether the user is close to falling asleep.⁶⁷

According to Appendices A and B paras 2, none of these are specifically mentioned by the companies, both of which keep it somewhat ambiguous, while NeuroSky did more than Emotiv. Emotiv mentions "EEG data" as a category, defining the electrical signals broadly, but giving examples of the equipment used for their collection and mentioning the presence of the sensory stimuli. Arguably still not enough, there is more information than what NeuroSky provides, which does not provide additional explanations.

Moreover, it is also possible to interfere other categories of data like medical conditions, sexual orientation, biometric information and political beliefs. EEG data could easily disclose this kind of information, especially by virtue of a wide palette of stimuli,⁶⁸ like the ones that are at the disposal of Emotiv and NeuroSky. Numerous mental diseases can be depicted from the variation of the electrical signals from the brain, like schizophrenia that can be identified in patients which have an increased level of the frequency bands delta and beta, and a lower activity in the alpha band.⁶⁹ Research from Karson and others has yielded that it only takes about 3 minutes of measuring EEG signals to be able to put the diagnostic.⁷⁰ A similar

⁶⁴ Ivy Wigmore, 'Black box AI', (TechTarget, August 2019), available at <<https://www.techtarget.com/whatis/definition/black-box-AI#:~:text=Black%20box%20AI%20is%20any,sense%2C%20is%20an%20impenetrable%20system>> accessed 4 September 2022.

⁶⁵ *ibid*

⁶⁶ See S. Rainey, K. McGillivray, S. Akintoye et al., (n. 2).

⁶⁷ N. Liu, C. Chiang and H. Chin-Chu, (n. 3).

⁶⁸ S. Rainey, K. McGillivray, S. Akintoye et al., (n. 2).

⁶⁹ J.J. Jewson and T.C. Thiagarajan, 'EEG Frequency Bands in Psychiatric Disorders: A Review of Resting State Studies', (2019), Volume 12, Issue 1, Front. Hum. Neurosc, available at <<https://doi.org/10.3389/fnhum.2018.00521>> accessed 30 June 2021.

⁷⁰ C. N. Karson, R. Coppola, D. G. Daniel and D. R. Weinberger, 'Computerized EEG in Schizophrenia', (1988), Volume 14, Issue 193, Schizophrenia Bulletin, available at <<http://psycnet.apa.org/record/2005-26897-010>> accessed 1 July 2021.

trajectory of brain signal measurement is followed for Alzheimer's disease and epilepsy,⁷¹ while Kanai and others have discovered that political beliefs can be intercepted just by analysing brain activity, with liberals and conservatives displaying different cognitive styles.⁷²

Moreover, whilst NeuroSky has set some mechanisms to ensure that an underage child has been granted parental approval in using its services as detailed in Appendix B para 15, Emotiv mentions that it does not offer its services to children under the age of 16, according to Appendix A para 14, but the company does not set any functioning mechanisms to restrict them from purchasing the EE headsets through its website. As such, the information collected could easily offer insights about children, which require a higher level of protection and care, one that the gaming manufacturer does not seem to be willing to ensure.

It is not only the diverse information that BCI technology can collect, but also the impressive quantity.

2.4.3. How much data is collected?

According to Appendices A and B, the companies do not collect more data than it is necessary for the purposes mentioned in paras 4 and, respectively, 3. However, the EE and MWM headsets disseminate an extraordinary amount of information because of the nature of the human brain and how the technology operates.

Humans have little control over their brain.⁷³ The organ is spontaneously and continuously active, displaying information involuntarily, as demonstrated by Martinovic's striking experiment, which presented to the world a consumer grade BCI used as a brain spyware. The users were presented with visual stimuli and, especially by virtue of the P300 paradigm, the authors were able to infer PIN numbers, dates of birth and bank information from their EEG signals.⁷⁴

As previously explained, stimuli can be designed to remain undetected and take place beyond the conscious perception of the individual. They can be tailor-made to each user so that the information generated by the brain reaches its full potential. As BCI technology is based on a neuroimaging technique, the information that is collected is massive by default. This happens because neuroimaging cannot offer access to independent brain signals, but gives a detailed overview of the anatomy of the brain itself and of its elaborate "patterns of inter-regional communication," offering data at the macro level about every process in the human brain.⁷⁵ The technique has also been referred to as the avant-garde of big data science, a trend that is known for its intrusiveness into the privacy of individuals.⁷⁶

Because of how BCI technology operates, it is impossible to limit the collection of brainwave data. The technology requires a calibration phase which is key to the translation of raw EEG

⁷¹ J. Engel Jr., D.E Kuhl, M.E Phelps and P.H. Crandall, 'Comparative localization of epileptic foci in partial epilepsy by PCT and EEG', (1982), Volume 12, Issue 6, *Annals of Neurology*, 529–37, available at <doi: 10.1002/ana.410120605> accessed 1 July 2021.

⁷² R. Kanai, T. Feilden, C. Firth and G. Rees, 'Political Orientations Are Correlated with Brain Structure in Young Adults', (2011), Volume 21, Issue 8, *Curr Biol*, 677–680, available at <<http://dx.doi.org/10.1016/j.cub.2011.03.017>> accessed 7 July 2021.

⁷³ H. Philips, 'Introduction: The Human Brain' (*New Scientist*, 4 September, 2006), available at <<https://www.newscientist.com/article/dn9969-introduction-the-human-brain/>> accessed 30 August 2021.

⁷⁴ I. Martinovic, D. Davies, M. Frank, et al., (n. 6).

⁷⁵ J. Shih, D. Krusienski and J. Wolpaw, (n. 23).

⁷⁶ J.D Van Horn and A.W. Toga, 'Human Neuroimaging as a "Big Data" Science', (2014), Volume 8, Issue 2, *Brain Imaging Behav.*, 323–331, available at <doi: [10.1007/s11682-013-9255-y](https://doi.org/10.1007/s11682-013-9255-y)> accessed 20 July 2021.

signals into output controls, and during which machine learning techniques are employed to enable the device to match the relevant signal to the command function.⁷⁷ On the one hand, when algorithms are employed, large sets of data need to be stored in order to train them.⁷⁸ On the other hand, algorithms employed in BCI devices need even more datasets for training as a consequence of the fact that the subject matter are the brain waves themselves, because every individual has a different neural response to the same stimulus due to the unique nature of the EEG signals (which will be discussed in the next chapter). As such, a generic brain signal cannot be stored and considered conclusive for every data subject and the only way in which it can operate to its full value is by collecting as much brain data as possible.⁷⁹

The large amounts of data are then stored and shared without adequate policies in place.

2.4.4. Where is the data stored and what are the sharing practices?

According to Appendices A and B, the information collected is continuously shared by Emotiv and NeuroSky with third parties that treat it like trivial data and stored on multiple platforms and databases for longer than necessary in practice, possibly in different jurisdictions.

Brain data collected by the MWM headsets is stored in the cloud or in data endpoints located in the United States until the user decides to delete his account. This also happens for data collected through the EE headsets, but Emotiv states that, in addition to the United States, data is also stored in other countries, without mentioning them, as seen in Appendix A para 8. NeuroSky does not provide the user with a choice regarding the storage location of data as, according to Appendix B para 10, users consent to the US as a storage place automatically when using its services. Storing data only for as long as necessary is impacted by the fact that purposes are broadly affirmed by the controllers. This can lead to the retention of datasets over an unreasonable period, as setting a purpose as specific as possible is interlinked with how much the data needs to be kept in order to achieve that purpose.⁸⁰

Emotiv and NeuroSky also admit sharing brain data with multiple third parties, as seen in Appendices A para 7 and B para 4, which subsequently store the personal information. The terms and conditions of the companies do not apply to these third parties and thus storage time will vary depending on the wish of each commercial actor, although such services can also be authorised and/or directly redirected by Emotiv, at least, as seen in para 10 of Appendix A. For instance, for the purpose of further facilitating the expansion of the neurogaming market, special BCI app stores and software development kits for open-source platforms have been created by both NeuroSky and Emotiv; and, since 2016, NeuroSky and Emotiv app stores comprise more than 100 applications. The open-development platforms where data may also be stored, are aimed at providing developers with access to all the raw signals that have been collected through BCI devices (hence offering them better insights into customers' profiles, and, more importantly for them, to the users' cognitive activities). The rationale is to enable them to create more tailor-made applications to the affective state of their customers (like increase/decrease difficulty of the video game according to the user's recorded capability and

⁷⁷ X. Huang, Y. Xu, J. Hua et al., 'A Review on Signal Processing Approaches to Reduce Calibration Time in EEG-Based Brain-Computer Interface', (2021), Volume 15, Front. Neurosci, available at <<https://doi.org/10.3389/fnins.2021.733546>> accessed 15 May 2022.

⁷⁸ J.D Van Horn and A.W. Toga, (n. 76).

⁷⁹ A. R. Gonzalez, 'EEG Signal Processing for BCI Applications', (2012), Volume 98, Issue 1, Human – Computer Systems Interaction: Backgrounds and Applications 2, 571-591, available at <DOI: 10.1007/978-3-642-23187-2_36> accessed 21 June 2021.

⁸⁰ Article 29 Working Party, Opinion 03/2013 on purpose limitation, ('WP 203'), 2013.

emotional state of the moment) through brain data, in order to increase sales on the market.⁸¹ Access to the personal information stored therein is granted through a common API for the developers, that is provided by the companies.⁸²

Further, collected data is transferred to other countries unknown to the users, with Emotiv, for instance, only mentioning the United States as a data endpoint. NeuroSky takes a similar approach, stating that limited actors have access to the data, but then mentioning multiple third parties in Appendix B, para 6. Moreover, as previously explained, the companies do not even mention the extent of information that can be inferred from EEG signals after processing and, thus, customers are unaware about what is shared during these practices.

Thus, although EEG data is shared with multiple actors and stored on various platforms, a clear retention policy is not in place. Similarly, Emotiv and NeuroSky should enforce adequate protection measures.

2.4.5. How do companies protect data collected through BCI?

The standards of protection enforced by the companies are low when considering the value of EEG data.

As a response to the increased level of neurocriminal activities like “malicious brain-hacking”, multiple scholars have already called for the introduction of a new generation of cybercrime: neurocrime.⁸³ There is an in-depth level of intrusion into a person’s life resulting from the processing of brain data, and the information can be easily mishandled if Emotiv and NeuroSky do not enforce an adequate level of protection. For instance, by purchasing the Emotiv SDK software, developers have, by virtue of a common API, unrestricted access to the raw EEG data collected by BCI devices in order to immerse themselves into the market demand for the gaming industry.⁸⁴ Attackers could use the neurodata to study and understand the correlation between the stimuli presented in a game and the information that they display, and in turn, adjust them and deploy more in order to maximise the amount of (sensitive) information that can be disclosed.

However, the security level set by Emotiv and NeuroSky is determined by measures that are only reasonable for the company from a financial perspective, like encryption, according to Appendices A and B paras 8. Conti and others found that regardless of the type of data encryption, the method is not effective when it comes to neuro cyber-attacks, with the perpetrators being able to intercept the information transmitted even in an encrypted format,⁸⁵ a similar conclusion reached by Martinovic and others.⁸⁶ The manufacturers even seem to try to avoid responsibility and accountability, should anything happen to the brain data; Emotiv through its statement regarding the effectiveness of the measures in Appendix A, para 8, and

⁸¹ S. Magids, A. Zorfas and D. Leemon, ‘A better way to drive growth and profitability’, (Harvard Business Review, November, 2015), available at <<https://hbr.org/2015/11/the-new-science-of-customer-emotions>> accessed 18 July 2021.

⁸² H.M de Arruda Leite, S.N. Carvalho, T.B Silva Costa et al., (n. 1).

⁸³ M. Ienca and R. Andorno, ‘Towards new human rights in the age of neuroscience and neurotechnology’, (2017), Volume 13, Issue 5, Life Sciences, Society and Policy, available at <<https://doi.org/10.1186/s40504-017-0050-1>> accessed 18 July 2021.

⁸⁴ *ibid*

⁸⁵ M. Conti, L.V Mancini, R. Spolaor and N.V. Verde, ‘Can’t you hear me knocking: Identification of user actions on android apps via traffic analysis’, (2015), Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, 297–304, available at <<https://doi.org/10.48550/arXiv.1407.7844>> accessed 20 July 2021.

⁸⁶ I. Martinovic, D. Davies, M. Frank, et al., (n. 6).

NeuroSky through its last comment regarding security of the transmission of data through the internet in Appendix B, para 8.

As such, brain data is treated like any other general category of information and, even in this case, whether the level of protection ensured is adequate is debatable.

2.5. Conclusion

This chapter provided a general overview of how the technology operates and aimed at illustrating the special features of BCI devices based on the EEG method, focusing on its application in the gaming field. In light of these, it assessed to what extent the terms of use governing the EE and MWM headsets reflect what happens in reality regarding the pre-collection practices, the quality and quantity of the data collected and how it is stored, shared and protected.

The key findings are:

- 1) BCI cannot limit the collection of brain data to only what is necessary, with the extent of the information ranges from the most private sphere to the most trivial. The amount is massive by default and the machine does not differentiate between the categories of data.
- 2) Users cannot be informed about what data is collected and understand the risks and threats involved in the processing operations, leaving them with no control over how their brain data is handled.
- 3) There is no retention period in place and data is stored in data collection endpoints in the US, the user having to consent to these operations.
- 4) Neurodata is constantly shared with third parties like any other piece of information and can even be sold in connection with a business deal, with no clear safeguards in place.
- 5) Because information like health condition, sexual orientation, political beliefs and many others can be inferred from brain data and the services are offered to children as well, there should be technical and organisational measures in place of the highest level in order to protect it. However, the companies avoid such responsibility and keep data security at a low level.

The question that now stands and will further be assessed is: If our society has adequately addressed these novel developments through the data protection law. The legal analysis will be assessed in the following chapter, with the European privacy legislation will be at the forefront of the discussion.

3. GDPR and Brain Information (BI)

3.1. Introduction

Although Emotiv's and NeuroSky's devices may offer a new and exciting gaming experience for vivid players, their practices severely threaten the privacy of their users. Their privacy policies should build trust and a sense of control to the customer over his own information.

However, the previous chapter has demonstrated that brain data is largely unprotected and mishandled, and that the data protection narrative of the companies regarding how their devices operate could not be true.

The focus of this chapter is to provide a legal analysis of the data processing practices in BCI by Emotiv and NeuroSky as explained in the previous chapter. It will illustrate the peculiar nature of brain data in light of which the potential challenges that BCI technology poses to the European data protection framework will be outlined, by using the privacy clauses of the two companies as points of reference. The first part assesses the legal status of brain data, whilst the second analyses the privacy policies of Emotiv and NeuroSky to check out to what extent their processing operations are GDPR compliant in practice and, as a result, determine how invasive are profiling and related decision making when carried through BCI technology, and law compliant in this context.

3.2. What is the legal status of brain data under the GDPR?

In order to adapt to the rapid technological developments, the GDPR is meant to be technology neutral, aiming to effectively protect personal data regardless of the technology and various technological techniques used/ that will be used in the future.⁸⁷ Although advances in neurotechnology in the future decades are going to leave policymakers confronting themselves with the privacy implications of brain monitoring and manipulation,⁸⁸ neurodata does not have a definition in the GDPR, nor is it specifically mentioned within the Regulation. In reality, the way it has been illustrated that BCI technology has special features, neurodata, similarly, distinguishes itself from the other categories of data due to certain particularities, leading to the need for different approaches, especially regarding the level of protection.

Neurodata has a dynamic, continuously changing nature, and a predictive characteristic, with its quality and the extent of information disclosed being uncontrollable.⁸⁹ First, the electrical signals collected from the brain are not static, in the sense that they can be interpreted in a way to reveal higher amounts of information and to a more in-depth level than intended based on the algorithms used and the expertise available. More specifically, while in their raw form EEG signals illustrate the physical characteristics of the brain, after further interpretation, they can reveal other trivial information about the individual, or even information of a more private nature, which is not immediately readable from their original raw status.⁹⁰ Second, as the previous chapter has explained, the data subject may not even be aware of such disclosures and cannot control them due to the involuntary activity of the human brain. Third, similarly to genetic data, whilst brain data can reveal diseases and physical/mental disorders, it can also disclose, in a predictive way, how prone individuals are to developing that disorder in the

⁸⁷ Ben Welford, 'What is GDPR, the EU's new data protection law?' (GDPR.EU), available at <<https://gdpr.eu/what-is-gdpr/>> accessed 22 April 2021.

⁸⁸ How should human mental capacity be regulated, or could solicitors one day be instructed to use a microchip to enhance their mental capabilities? See K. Ahadi, 'Neurotechnology, law and the legal profession', (The Law Society, 9 August, 2022), available at <<https://www.lawsociety.org.uk/topics/research/how-will-brain-monitoring-technology-influence-the-practice-of-law>> accessed 20 August 2021.

⁸⁹ Multiple experiments have demonstrated its peculiar characteristics. See, for example, D. Vidaurre, R. Abeyesuriya, R. Becker, et al., 'Discovering dynamic brain networks from big data in rest and task', (2018), Volume 180, NeuroImage, 646-656, available at <<https://doi.org/10.1016/j.neuroimage.2017.06.077>> accessed 20 August 2021.

⁹⁰ J. Shih, D. Krusienski and J. Wolpaw, (n. 23).

future.⁹¹ Moreover, the predictive characteristic can even go beyond the medical sphere, and potentially also predict behaviour patterns. Last, the closeness of the link between the brain data and the individual is unique. EEG signals present a unique link to the data subject, one that cannot be broken due to their characteristic of being inherently identifiable, showing a function that is specific to someone's brain only.⁹² Because the signals are a reflection of internal mental tasks that are individual dependent, they cannot be copied or reproduced.

The second chapter has outlined the fact that NeuroSky and Emotiv treat brain data like any other type of trivial information, but this part will assess if it qualifies for special protection under the GDPR in light of its special characteristics, and whether the companies should treat it accordingly. Additionally, this part will also explain the challenges that it brings to the concept of anonymisation, which will be seen in practice in the second part, through the discrepancy between their privacy policies.

3.2.1. Defining personal information

EEG signals qualify for protection under the GDPR, but their raw form and direct collection from the brain raise challenges to the definition of personal data under the Regulation, with its application not being obvious from the outset.

According to Article 4, personal data relates to information about an individual whose identity is either manifested clearly (the individual is identified), or that can be discovered by using additional information (the individual is identifiable). Art. 4(1) also mentions that identifiability of the individual can happen directly or indirectly, through an identifier.

At the time of assessing whether an individual is “identified or identifiable”, “all means that are reasonably likely to be used” in the identification process of the individual have to be taken into consideration, including the technology that is available and future developments in the field.⁹³ An important characteristic of identifiability is that the identity of the individual does not need to be determined in the narrow sense anymore, but that it is enough to be able to single out/categorise the individual from others on the basis of a criteria in order to be able to attribute certain decisions to him or her.⁹⁴ While a name, for instance, is a self-explainable example for the potential direct establishment of identity, indirect identifiability presents more ubiquitous cases. The level of abstractness goes as far as considering “protocol addresses, cookie identifiers or even radio frequency identification tags” indirect identifiers as, when combined with *other information*, can lead to the indirect identifiability of an individual.⁹⁵

But not any hypothetical situation when identifiers are combined with EEG data, in this case, will actually lead to the identifiability of the individual.⁹⁶ The reasoning in the *Breyer case* shed some light on this issue.⁹⁷ The European Court of Justice determined that an IP address is considered personal data under the data protection framework, when the IP address combined with additional information represents a means that is likely reasonably to be used for the

⁹¹ The Committee on Science and Law, ‘Are Your Thoughts Your Own?: Neuroprivacy and The Legal Implications of Brain Imaging’, (New York City Bar, 1 June, 2005), available at <<https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/are-your-thoughts-your-ownneuroprivacy-and-the-legal-implications-of-brain-imagingpdf>> accessed 26 November 2021.

⁹² *ibid*

⁹³ Recital 26 of the GDPR.

⁹⁴ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, (‘WP136’), 2007.

⁹⁵ Recital 20 of the GDPR.

⁹⁶ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, (n. 94).

⁹⁷ Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016].

identification of the data subject.⁹⁸ As such, identifiability is assessed on a case-by-case basis and there are more factors that need to be taken into account when considering the likelihood of identification by combining identifiers.⁹⁹ Although not an exhaustive list, factors that help with determining it, and which are also helpful in this situation, are: the processing purpose, the cost and effort involved in identification, gains of the controller resulting from the processing activities, what is at stake for the data subject, the effectiveness of the measures implemented to maintain anonymity and the technology and future technological developments.¹⁰⁰

EEG data is acquired, among other purposes, also to customise the game as much as possible to provide the player with the best experience. To be able to adjust each game based on preferences, the BCI needs to categorise the brainwave signal and recognize it as belonging to a certain user, inherently basing its functionality on identifiability.¹⁰¹ The power that neurodata gives to its possessor has already been discussed, as well as the immense risks for the data subjects. The effectiveness of anonymisation techniques in the context of neurodata will be assessed in the next section, but their potential is relatively low. Regarding the technological realm, data processing technologies like data mining techniques and pervasive technologies develop at a great speed.¹⁰² Consequently, although a data set may not have been considered identifiable when data processing commences, the increased availability of more sophisticated new technological tools may turn or make the data appear to have been identifiable all along.¹⁰³ A welcomed clarification, especially for this case, is the fact that personal data is defined broad enough to contain all potential ways of identification and all degrees of identifiability.¹⁰⁴ As such, an individual is considered identifiable by virtue of EEG signals.

An additional challenge that EEG data brings to the GDPR is its raw form, raising questions whether it would fall under the term “any information” protected by the Regulation. Assessments of the meaning of this term were rather reduced in the past, perhaps because it was considered self-evident.¹⁰⁵ And while its scope is indeed very broad, advanced algorithms, computing techniques and data analytics, all of which are represented through codes, have come to challenge not the kinds of information that would fall under “any information”, but the meanings of the term “information” *per se*.¹⁰⁶ In the case of BCI technology, albeit the processing of the EEG signals results in the disclosure of data that would undoubtedly be considered “any information,” it is not evident from the outset that EEG signals in their raw

⁹⁸ *ibid*

⁹⁹ Recital 26 of the GDPR.

¹⁰⁰ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, (n. 94).

¹⁰¹ See F. Lotte, F. Larrue and C. Muhl, ‘Flaws in Current Human training Protocols for Spontaneous Brain-Computer Interfaces: Lessons Learned from Instructional Design’, (2013), Volume 7, *Frontiers in Human Neuroscience*, available at <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3775130/>> accessed 10 October 2021.

¹⁰² N. Purtova, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’, (2018), Volume 10, Issue 1, *Law, Innovation and Technology*, 40-81, available at <<https://dx.doi.org/10.2139/ssrn.3036355>> accessed 10 October 2021.

¹⁰³ See B.J. Koops, ‘The Trouble with European Data Protection Law’, (2014), Volume 4, Issue 4, *International Data Privacy Law*, available at <doi: 10.1093/idpl/ipu023> accessed 20 October 2021.

¹⁰⁴ European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European data protection law*, (n. 7).

¹⁰⁵ See N. Purtova, (n. 102). Literature on the interpretation of “any information” is not significant.

¹⁰⁶ See R. Gellert, ‘Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?’, (2020), Volume 16, Issue 1, *Regulation and Governance*, 156-176, available at <<https://doi.org/10.1111/rego.12349>> accessed 28 October 2021. It shows that concepts enshrined in data protection law are in stark contrast with machine learning.

form would as well. This is because, in their initial phase, at collection, they are illustrated through lines and waves that are in an unreadable form before interpretation, as previously explained. Nonetheless, according to Article 29 WP, the format or form of the information is not significant, and information could even represent “alphabetical, numerical, graphical, photographic or acoustic data,” if the other requirements from the definition are satisfied.¹⁰⁷ Taking into consideration the extensive meanings attached to the term, EEG signals, represented through waves, fall under “any information” as required by the data protection framework.

Albeit not an obvious case, after a close analysis it is clear that brain data qualifies for protection under the GDPR. However, the level of protection awarded under the Regulation is challenged in this context.

3.2.2. Sensitive data

Although brain data is particularly sensitive, its peculiar characteristics challenge the application of the definition of special categories of data. Therefore, it ends up being treated like a general category of personal data of trivial nature by commercial actors like Emotiv and NeuroSky.

The European legal framework grants enhanced protection to personal data that, because of its nature, may pose a significant risk to the data subjects. As such, although not an exhaustive list, Art. 9(1) provides the categories of data that are considered sensitive (special), and can be processed only under limited conditions, being subjected to a prohibition principle.¹⁰⁸

The electrical activity of the brain is captured under the form of waveforms that, when illustrated on the screen after collection, is exactly what they represent: mere waveforms. As such, the verbatim a word-for-word translation of the meaning of EEG signals is electric cortical activity, which is not considered sensitive data *per se*, as it is not mentioned under Article 9 of the GDPR. However, although not special data from the point of collection, EEG signals have the potential of revealing sensitive information after being processed, including but not pertaining to: health data, political beliefs and personality traits.¹⁰⁹ It is worth mentioning that for the interference of complex medical conditions and other sub-categories, special algorithmic processes need to be employed, as well as more time, effort and specialised knowledge, as previously explained. However, the following line of reasoning illustrates that Emotiv and NeuroSky still infer and process at least health data, which is protected under Art. 9.

Whereas, as explained, a complete medical examination only by using the headsets cannot be provided, diagnosis of mental health conditions is not so difficult to infer. For instance, slight variations in the beta wave can point to schizophrenia.¹¹⁰ According, for instance, to para 4 in Appendix A, Emotiv, compares the EEG signals from different players to improve the quality of its service. The company may not even need to employ special algorithms to infer medical conditions about certain individuals but could reach this conclusion only by comparing their brain waves and realising that they are not the same, but that some present such variations and, afterwards, reach the diagnosis. Based on this judgement, it is highly likely that the companies

¹⁰⁷ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, (n. 94).

¹⁰⁸ *ibid*

¹⁰⁹ I. Martinovic, D. Davies, M. Frank, et al., (n. 6).

¹¹⁰ C. N. Karson, R. Coppola, D. G Daniel, D. R. Weinberger, (n. 70).

infer other types of sensitive information through this technique, as well, without the need to employ special algorithms.

However, because neurodata is not mentioned under Art. 9, it is processed under the requirements of personal data. The general reluctance to categorise EEG data as sensitive data may be attached to the fact that EEG data does not always disclose information of sensitive nature under the scope of Article 9 due to its dynamic nature, but, for instance, it can also reveal data about an individual's general preferences only, which is treated as a general category of personal data of trivial nature. Greater clarity is needed in this area as, consequently, BCI manufacturers like Emotiv and NeuroSky remain silent about processing sensitive data and treat brain data to a lower standard of protection.

3.2.3. Data processing

Although EEG data falls under the definition of “personal data,” to be protected by the Regulation, Art. 4(2) states that such information has to be processed. The GDPR takes a broad approach as to what “processing” means, with Art 4(2) referring to it as “...any operation or set of operations which is performed on personal data...” either done “wholly or partly by automatic means.” As such, data processing relates to most of the operations applied to personal data, which include collection, interpretation, analysis and storage of such data, practices which are carried out by both NeuroSky and Emotiv.

Thus, both companies are processing EEG signals, which, although not obvious from the outset, are personal data. However, the application of “anonymisation” is more controversial in this case.

3.2.4. Anonymisation: outdated when it comes to neurodata?

One of the inherent characteristics of brain data previously illustrated is its unique and close link with the individual. This peculiarity, combined with the fast technological developments and the increased ability to easily combine multiple datasets might always enable the re-identification of individuals through brain data.

According to the GDPR, anonymization is the process by which all identifying elements are eliminated from a set of personal data, such that the data subject is not identifiable anymore.¹¹¹ Consequently, the data is not considered personal data anymore and the Regulation does not apply.¹¹²

Article 29 Working Party has analysed different anonymisation techniques based on their effectiveness and it has concluded by acknowledging that their suitability is decided on a case-by-case basis.¹¹³ To ensure anonymity, the identifying elements from neurodata sets would have to be excluded,¹¹⁴ which may be impossible in the case of EEG signals, given their distinctiveness and unique link with the data subject. As previously explained, brain data indicates patterns of the human brain and its activity that are singular for every individual, regardless of the fact that they are engaged in the same activity.¹¹⁵ The case is very similar

¹¹¹ See Recital 26 of the GDPR.

¹¹² *ibid*

¹¹³ Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, (‘WP216’), 2014.

¹¹⁴ Recital 26 of the GDPR.

¹¹⁵ A. R. Gonzalez, (n. 79).

(albeit still different) with biometric data.¹¹⁶ The scepticism stems from the fact that, removing the identifiers from the biometric datasets in order to declare anonymity goes against the very nature of biometric data, which is full of bulks of data points that are unique.¹¹⁷ This case is similarly controversial, the disagreement surrounding the anonymisation of brain data being illustrated through the discrepancies between the approaches of NeuroSky and Emotiv, which will be more extensively discussed in practice in the next part. According to Appendix A para 5, on the one hand, Emotiv does not claim to anonymize neurodata anymore, but that it uses pseudonymisation instead, whereas NeuroSky stands by its approach, as seen in Appendix B para 2.1.

The threshold for the anonymisation techniques remains the irreversibility of the process, taking into account the risk of re-identification.¹¹⁸ In this respect, as a rule of thumb, the more attributes are present in a data set, the higher the possibility for a match, and less likely for anonymization to have proven effective.¹¹⁹ Through advanced algorithms, researchers were able to re-identify individuals by using only five pieces of information chosen randomly from credit card metadata, whilst another study demonstrated that it is possible to re-identify 95 percent of individuals from a data set by using only four spatio-temporal points.¹²⁰ Assessing what identifiers are present in EEG waveforms, these can be characterised, to only name some, based on “location, amplitude, frequency, morphology, continuity (rhythmic, intermittent or continuous), synchrony, symmetry, and reactivity.”¹²¹ In addition to the low chance of irreversibility because of the high presence of identifiers, two factors are definitive in deeming de-identifiability of neurodata impossible: the fact that the neurodata is constantly collected and easily combined with other datasets and the rapid developments that happen in the technological realm.

As previously explained, the experience provided by BCI-enabled games and the quality improvement sought by manufacturers rely on the collection of large sets of neurodata, which takes place whenever the user accesses the headsets. As such, although previous neurodata sets may have been “anonymised” by NeuroSky, new personal information is constantly being collected by the devices and stored to provide a big picture of the mental processes of the player. According to Appendix B para 4, NeuroSky also shares neurodata for research purposes after being anonymised (assuming it is working effectively). Following its lead, extensive databases containing anonymised neurodata from a multitude of BCI-devices and apps on the market are being increasingly made available for research purposes.¹²² This data can easily be combined with information that can be found on social media, for example, or other databases.

¹¹⁶ See J. Banda, ‘Inherently identifiable: Is it possible to anonymize health and genetic data?’, (IAPP, 13 November, 2019), available at <<https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/>> accessed 26 November 2021. And just like biometric data, brain data is also inherently identifiable.

¹¹⁷ N. Lomas, ‘Researchers spotlight the lie of ‘anonymous’ data’, (TechCrunch, 24 July, 2019), available at <<https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/>> accessed 29 November 2021.

¹¹⁸ Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, (n. 113).

¹¹⁹ Estimating the success of re-identifications in incomplete datasets using generative models. See N. Lomas, (n. 117).

¹²⁰ *ibid*

¹²¹ C.S. Nayak and A.C. Anilkumar, ‘EEG Normal Waveforms’, (2022), National Centre for Biotech. Info., available at <<https://www.ncbi.nlm.nih.gov/books/NBK539805/>> accessed 20 November 2021.

¹²² BCI research regarding its potential applications has experienced a significant exponential growth. See J.J. Daly and J.E. Huggins, ‘Brain-Computer Interface: Current and Emerging Rehabilitation Applications’, (2015), Volume 96, Issue 30, Arch. Phys. Med. Rehabil., available at <doi: 10.1016/j.apmr.2015.01.007> accessed 20 November 2021.

As such, as the amount of data publicly made available grows, combining different databases becomes a day-to-day practice¹²³, and so does the likelihood of being able to link any piece of information to a person without “exercising an unreasonable amount of time and effort, or incurring any costs.”¹²⁴

Constant and fast advances in computing also have a crucial role in redefining what techniques are rendered suitable for anonymisation. Stripping a data set of its markers was considered enough from a data protection perspective some time ago.¹²⁵ However, the evolution of machine learning techniques and, reportedly, classification techniques in particular, which is one of the main algorithm techniques employed in BCI, continuously redefine the effectiveness of anonymisation, which is exactly the debate centred around identifiability from section 3.2.1. Related to this aspect, as stated in the previous discussion as well, regardless of what methods are explored to break the link between the individual and neurodata, this may never be possible due to the fact that it illustrates mental processes associated with a specific person. Afterall, EEG signals are rapidly emerging as a new means for authentication because they are inherently identifiable and unique.¹²⁶

Therefore, the increased ability to easily combine multiple datasets, along with the fast technological advancements and the uniqueness of the EEG signals seem to suggest that anonymisation is inadequate in this situation and that brain data should be considered personal data regardless, an approach even supported by Emotiv. Lastly, there is one thing to be considered: brain data has a particularly sensitive nature; and since anonymization cannot be guaranteed to be fully effective at this moment, perhaps BCI companies like NeuroSky, who takes a different approach than Emotiv, should steer clear from fully relying on it. Afterall, as Hallinan puts it, “What may be anonymous today, may turn out to not be anonymous tomorrow.”¹²⁷

Thus, brain data is considered personal data under the GDPR and processed by NeuroSky and Emotiv accordingly, as set in their privacy policies.

3.3. To what extent can current BCI practices be considered compliant to the GDPR?

The practices of the EEG and MWM headsets threaten the privacy of the users as explained in the previous chapter. Whilst the first part of this chapter assessed the peculiar characteristics of brain data and its legal nature, this part will discuss them in the context of the following data protection principles, including:

- Lawfulness

¹²³ K. Verslype, ‘Linking Together Personal Data in the Era of Big Data & GDPR’ (Smals Research, 18 March, 2018), available at < <https://www.smalsresearch.be/data-archipelago-and-gdpr/> > accessed 30 November 2021.

¹²⁴ Factors that are taken into account when assessing the likelihood of re identification. See Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, (n. 113).

¹²⁵ J. Banda, (n. 116).

¹²⁶ S. Zhang, L. Sun, X. Mao, C. Hu and P.Liu, ‘Review on EEG-Based Authentication Technology’, (2021), Volume 2021, Comput. Intell. Neurosci., available at <doi: 10.1155/2021/5229576> accessed 27 November 2021.

¹²⁷ D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 11).

- Transparency
- Data minimisation
- Storage limitation
- Data security
- Purpose limitation
- International transfers of data
- Third-party sharing of data
- Profiling and decision making based on profiling

Further, the privacy policies of NeuroSky and Emotiv according to each of them will be assessed.

3.3.1. Lawfulness and transparency

According to Appendices A para 6 and B para 3, Emotiv and NeuroSky rely on consent or legitimate interest for processing brain data for their purposes. Considering the findings regarding their pre-collection practices, the requirements for validity of consent are not fulfilled (excepting for the requirement for the withdrawal of consent), and, similarly, the transparency principle cannot be complied with. Regarding the requirement of legitimate interest, it is debatable whether it would represent an appropriate legal ground, but the balancing test would incline to suggest otherwise, for now.

The data protection legal framework requires data processing to be done, among others, in a lawful and transparent way under Art. 5(1). Lawfulness is satisfied when the processing operations are based either on consent or on other legitimate ground(s) enshrined in Art. 6(1), like “legitimate interest”. According to Art. 4(11), for a consent to be valid, it must be freely given, specific, informed and unambiguous, with the data subject being granted the right to withdraw his consent at any time, whilst Art. 6(1)(f) allows for the processing of personal data if it is “necessary for the purposes of the legitimate interests pursued by the controller...except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject...” Finally, Art. 12 provides that the transparency principle imposes an obligation on the controller to keep data subjects informed regarding how their personal information is used. As such, the controller must provide explanations about processing operations in an easily accessible way and clear and plain language to enable data subjects to fully understand the risks, safeguards, rights and rules that are involved in the processing activities.¹²⁸

The way the transparency and simplicity concepts during pre-collection practices are not respected, consent to the processing activities cannot be informed in the processing practices of NeuroSky and Emotiv. The data subject is not made aware about the diversity and variety of information that is collected about him in the aftermath of the translation of the electrical bio signals. Additionally, AI tools are responsible for extracting and interpreting scientific expertise about the function of the human brain. As such, the player will never be able to comprehend the degree of risk arising from the processing activities or the consequences involved. Explaining cognitive activities and their impact in a plain and intelligible language

¹²⁸ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, (‘WP260’), 2017.

to ensure that any users would understand the severity of the situation, as imposed by the transparency principle,¹²⁹ would be impossible.

Consent also needs to be freely given, meaning that the data subject has to be presented with a real and free choice.¹³⁰ However, an individual also has very little voluntary control over his mental processes, with the majority of cognitive activity taking place because of practices that are largely unconscious to the human mind anyway.¹³¹ As such, the user is likely to disclose information without his knowledge or that he is not even aware of.

Consent is also not specific to the processing purposes of Emotiv and NeuroSky. However, consenting to the collection of EEG signals for specific and granular purposes is not feasible anyhow because of their special nature previously explained. Due to their dynamic nature, it is only after the translation and interpretation that brain waves are given meaning, not during collection. Consequently, it is impossible to respect the wish of the data subject regarding his consent to the collection of data for only certain purposes, as it is impossible to discriminate between the information collected prior to when the signals have been interpreted.

Consent needs to be unambiguous, meaning that agreement to the processing operations has to be indicated through a statement or a clear affirmative action and actions like silence, pre-ticked boxes or inactivity will not suffice.¹³² According to Appendix A para 1, once the customer accesses or uses the services provided by Emotiv, although having not clicked “I accept Emotiv’s privacy policy” the customer gives express consent to the processing of EEG data, with NeuroSky taking a similar approach. As per the EDPB, a “clear affirmative act” regards a deliberate action that has been taken to consent to the particular processing, which should leave no doubt about the intention of the data subject.¹³³ But express consent cannot be considered valid, since it is granted through the customer’s mere utilisation or access to the services, which is highly likely to fall short of the high threshold set by the EDPB.

Last, both Emotiv and NeuroSky market their products to children, processing their personal data. According to its privacy policy, Emotiv does not knowingly process the personal data of children and neither does it intend to. However, as per the EDPB guidelines, when using consent as a legal basis when providing information society services to children, the controller has to make reasonable efforts to ensure that the user is indeed over the age of digital consent to access its services, efforts which are expected to be proportionate with the nature and the risks stemming from the processing activities.¹³⁴ In light of the special nature of neurodata previously illustrated, conducting further checks to ensure that children are not accessing the service should be mandatory, although none of the companies seem to do so.

Although consent cannot be valid in this case because its requirements are not satisfied, Emotiv also mentions legitimate interest as a legal ground for processing brain data for profiling purposes in para 4 of Appendix A.¹³⁵ But because brain data reveals sensitive information, processing for profiling purposes should not take place on this basis, but on the basis of express

¹²⁹ *ibid*

¹³⁰ Recital 42.

¹³¹ A. Stopczynski, D. Greenwood, L.K. Hansen and A.S. Pentland, (n. 56).

¹³² European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, 2020.

¹³³ *ibid*

¹³⁴ European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, (n. 132).

¹³⁵ However, profiling practices will be assessed more extensively in section 3.3.5 and only mentioned in this section.

consent.¹³⁶ However, even so, the legitimate interests of the companies do not override the fundamental rights and interests of their customers as required by the balancing test.¹³⁷ This is because, taking into consideration the information that brain data discloses about its possessors, using this type of information is excessive in this context and there is a significant intrusion into their customers' lives, which can have an undue impact on their rights. As such, right now, this will most likely tip the balance in favour of not allowing Emotiv and NeuroSky to use the legitimate interest as a legal ground in processing brain data.

Taking these into consideration, consent should not be used as a legal basis by Emotiv and NeuroSky for their processing activities, as it does not adequately safeguard individuals. Legitimate interest could be used by Emotiv and NeuroSky as a legal ground if more safeguards would be ensured and the risk of interference with their customers' rights would be reduced,¹³⁸ with recommendations being provided in the last chapter.

3.3.2. Purpose limitation

The principle of purpose limitation under Art. 5(1) provides that personal data has to be collected only for well-defined and specific purposes, further processed for specified purposes and in a manner that is not incompatible with the original ones that it has been collected for.

The fundamental incompatibility with this principle lies in the fact that BCI manufacturers (incl. Emotiv and NeuroSky and companies activating in the gaming industry in general) set a broad purpose for their operations, disproportionately increasing the collection and processing of information to gain commercial interests.¹³⁹

In particular, section 3.2.2 has illustrated that EEG signals have the potential of revealing health data. This type of information reaches Emotiv and NeuroSky because BCI technology operates by recording any electrical activity taking place in the human brain. Thus, defining specific purposes in this situation would be useless anyhow, since all the EEG signals recorded are processed, regardless of the purposes set. Additionally, a specific purpose would mean that users will have to be informed more thoroughly and precisely about each piece of personal information that will be collected a priori to the process.¹⁴⁰ But the previous section has explained that providing the user with such explanations is impossible in BCI practices.

Therefore, there is a clear legal incompatibility between the purpose limitation principle and the way the EE and MWM headsets process personal data, as they also collect information that should not be used for the purposes mentioned by Emotiv and NeuroSky. The principle is tied to data minimisation, as they both oversee collection practices and hinder unreasonable and excessive amounts of data.¹⁴¹ As such, the latter will be further assessed, alongside storage limitation and data security.

¹³⁶ European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, (n. 132).

¹³⁷ Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014.

¹³⁸ *ibid*

¹³⁹ See V.M. Schonberger, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation', (2016), Volume 17, The Columbia Science & Technology Law Review, available at <https://www.researchgate.net/publication/303665079_Regime_Change_Enabling_Big_Data_Through_Europe%27s_New_Data_Protection_Regulation> accessed 5 November 2021. The authors assessed the privacy policy of Facebook and reached this conclusion.

¹⁴⁰ Article 29 Working Party, Opinion 03/2013 on purpose limitation, (n. 80).

¹⁴¹ European Union Agency for Fundamental Rights, Council of Europe, Handbook on European data protection law, (n. 7).

3.3.3. Data minimisation, storage limitation and data security

The core of the data minimisation principle requires controllers to process data only to the extent that it is “adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed” under Art. 5(1). But the findings from chapter two have already indicated that the amount of data collected cannot be limited.

Both companies, according to Appendices A and, respectively, B, state that they collect only the relevant and necessary data for the purposes mentioned in Appendices A para 3 and B para 4. But to minimise the collection of data, the personal data would have to be already “triaged” before collection. This would ensure that a smaller quantity, only strictly necessary to that specific purpose, is recorded, which goes against the functionality of BCI technology, that records any involuntary and uncontrollable mental response for further interpretation into readable form, as explained in the previous section.

Regarding storage, the principle of storage limitation imposes an obligation to delete or anonymise personal data as soon as it no longer serves the purposes for which it was collected under Art 5(1). NeuroSky states in Appendix B para 12 that after fulfilling the purposes for which the data was collected, it anonymizes and keeps such data *indefinitely*. However, as previously shown, anonymization of EEG data is highly likely to be ineffective in this case. When shared with game developers, the EEG data is to be stored on open-development platforms that lack an appropriate level of security, and for an unspecified amount of time. There are market standards that apply to practices regarding performance of BCI-based games, physical safety of the devices, their reliability, and many others, just as they would be applied to a traditional video game. However, albeit this general precaution, there are no clear effective guarantees in place when it comes to user’s privacy and safety, as no review process, and technical protection or policies are ensured.¹⁴² This means that game developers may have unlimited access to the platforms and full control over the data that is collected at any stage of the BCI-cycle. Even more important is the fact that platforms are immunised from the applications that are submitted by game developers, so manufacturers of BCIs are not encouraged to report or protest other applications that may be abusive from a privacy perspective.¹⁴³

Therefore, the application of the principles of data minimisation, storage limitation and data security are less effective in the BCI environment. There is no clear retention policy in place and personal data is transferred to the US and stored there in data endpoints.

3.3.4. International data transfers

To provide sufficient protection of the rights and freedoms of data subjects, the GDPR aims to ensure the same level of protection as within and outside the EU. These transfers are allowed only if the third country ensures a level of protection that is adequate, or if appropriate safeguards like data subject rights and remedies are provided, through means like standard data protection clauses or binding corporate rules.¹⁴⁴

According to Appendix B para 10, NeuroSky transfers EEG data to the United States, while Appendix A para 8 states that most EEG data is stored by Emotiv “in limited access servers located in the United States.” Under EU law, NeuroSky and Emotiv may transfer personal data

¹⁴² T. Bonaci, R. Calo and H. Chizeck, (n. 19).

¹⁴³ *ibid*

¹⁴⁴ Recital 101 and Recital 116 of the GDPR.

from the EU to the US can be based on either an adequacy decision granted by the European Commission, under Art. 45, or, if this is not the case, appropriate safeguards are provided. As a last resort, derogations are also available on rare occasions. While the “Safe Harbour” framework allowing for transfers of data to the US has been declared invalid by the ECJ, “EU-US Privacy Shield” was initiated in 2015, but soon ran into trouble.¹⁴⁵ To date, some progress has been made, but nothing is set in stone now.

NeuroSky and Emotiv have been active in the BCI-game field for a long time. If the two companies were able to continue to legally transfer data to the US, they must have resorted to the second approach, ensuring that appropriate safeguards of data subjects’ rights and remedies were provided under Art. 46. These can be established by binding corporate rules and standard contractual clauses, among others.¹⁴⁶ Additionally, even in the absence of the aforementioned, under Art. 49, personal data transfers may still be justified in certain circumstances, among which, when the data subject “gives explicit consent for the data transfer.”

Through the language illustrated in Appendices A para 1 and B para 10, both NeuroSky and Emotiv seem to use the derogation of consent as the basis for international transfers to the US. However, the information provided about international transfers is not publicly made available, and what is mentioned in their privacy policies is rather ambiguous. But section 3.3.1 showed that the validity of consent cannot be fulfilled when used as a legal ground in BCI processing practices, including in international transfers, especially since the information transferred is highly sensitive.

One could also assume that the two companies based their transfers on binding corporate rules, because the EU allows for this basis if the transfer takes place within the same group of enterprises that are part of a joint economic activity under Art. 47. For binding corporate rules, Art. 47 provides that, to be approved by the supervisory authority, they must contain all the fundamental data protection principles, comply with certain formal requirements, and expressly grant enforceable rights for data subjects. However, whilst their privacy policies cover the fundamental principles and rules enshrined in the GDPR, their application is less effective in this context, as explained. Thus, binding corporate rules could be the basis of such transfers, but it is debatable whether they are appropriate, considering the findings so far.

3.3.5. Profiling and profiling-based decision making

The fact that brain data is treated by Emotiv and NeuroSky only as a general category of personal data influences how profiling practices are carried out, as the processes are treated differently under the GDPR when sensitive data is involved. This section will assess and compare both cases, how the companies currently treat and should treat these practices, considering the special nature of brain data.

Aggregated data can reveal an impressive amount of information. By virtue of profiling, the inferences and predictions from a dataset are now automated.¹⁴⁷ There are three circumstances in which profiling is involved under Article 22(1) of the GDPR, namely: general profiling; decision-making based on profiling; and solely automated decision-making, including profiling, which produce legal effects or similarly significantly affect the data subject.¹⁴⁸ In the

¹⁴⁵ European Union Agency for Fundamental Rights, Council of Europe, Handbook on European data protection law, (n. 7).

¹⁴⁶ Article 46 and Article 47 of the GDPR.

¹⁴⁷ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (n. 22).

¹⁴⁸ *ibid*

following, only the former two will be analysed in the gaming BCI context (with the reason for exclusion of the 3rd explained below).

There are general benefits of profiling and decision making based on profiling, such as heightened efficiencies and savings of resources. They provide an opportunity to segment markets easier and better, enabling businesses to tailor their services to their clients, which can be aligned to their needs and preferences.¹⁴⁹ The EU data protection framework tries to balance the business interests of companies with the protection of the data subjects.¹⁵⁰

Profiling is defined in Art. 4(4) as a “procedure which may involve a series of statistical deductions ... often used to make predictions about people,” based on data obtained from various sources. It consists of three elements: an automated form of processing; carried out on personal data; for the objective of evaluating personal aspects about a natural person. The GDPR stresses that profiling is automated decision making used for “evaluating” in the sense that it can help “analyse” *or* “make predictions,” with mere classification not sufficient.¹⁵¹

Processing sensitive data for profiling purposes (which is the case here) is, by default, not allowed unless certain conditions are met. The controller must ensure that: (a) the processing is not incompatible with the original purpose; (b) there is a lawful basis for the processing of the special category data; and (c) data subjects are informed about the processing. The original purpose for the processing of EEG signals is to enable customers of Emotiv and NeuroSky to play games through the EE and MWM headsets (i.e delivering the service), while the second purpose, which implies further processing, is the improvement of services and delivering the best customised experience for the player as detailed in Appendix A para 4, which effectively translates into “profiling practices”. Since there is a high possibility that data subjects would not reasonably expect extremely sensitive information like health data to be further used by Emotiv or NeuroSky for profiling and there are great risks and negative consequences involved in this processing, the latter purpose should not be considered compatible with the original purpose under the compatibility test.¹⁵² Explicit consent cannot be considered valid in this context, as previously outlined and, regarding the information provided, it should not only disclose that profiling will take place, but it should also contain information regarding the logic involved in the practice and the consequences for individuals resulting from the processing.¹⁵³ Turning to the privacy policies of Emotiv and Neurosky, Appendix A para 4 and Appendix B para 3 illustrate that the information provided to the customer about profiling practices carried out is minimal. Both companies use EEG to profile its customers, but this can only be interpreted from the broad language used, as the term “profiling” is never specifically mentioned. No clear explanation is given about the logic involved in profiling, how the algorithms work, or about what factors are used to create the profile. Considering these, profiling and profiling-based decision making should not be allowed in this context, taking into consideration the special nature of brain data and the sensitivity of information.

However, because brain data is not treated as a special category of data under the GDPR and Emotiv and NeuroSky handle it only as a general category of personal data; the companies take

¹⁴⁹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (n. 22).

¹⁵⁰ Lee Matheson, ‘WP29 releases guidelines on profiling under the GDPR’, (IAPP, 18 October, 2017), available at <<https://iapp.org/news/a/wp29-releases-guidelines-on-profiling-under-the-gdpr/>> accessed 20 October 2022.

¹⁵¹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (n. 22).

¹⁵² Article 29 Working Party, Opinion 03/2013 on purpose limitation, (n. 80).

¹⁵³ Article 13 of the GDPR.

the following approach: under the GDPR, when sensitive data is not involved, profiling and related decision making can be carried out as long as there is a lawful basis for the processing and the principles enshrined therein are respected.¹⁵⁴ As previously explained, the legal basis of consent is not valid in this situation, but the companies, alternatively, base their processes on another legal ground: legitimate interest (which could not be used if brain data would have been treated as sensitive data), lowering the standard of protection. In this context, of the utmost importance is Art. 21, which provides that the controller must specifically outline the provision of the right to object the processing of data (including profiling). Moreover, when such processing (including profiling) is related to direct marketing purposes, the right is unconditional, i.e., balancing of interests is not necessary anymore, with the controller being obliged to respect the wish of the individual with no further questioning about the reasons behind the objection under Art. 21. The right can be exercised whenever the data subject wishes and free of charge.¹⁵⁵ However, the fact that NeuroSky and Emotiv use ambiguous wordings in their privacy policies when informing data subjects about the presence of profiling, and the complete silence about related decision making greatly affects the ability of data subjects to exercise this right, as, consequently, these practices occur largely without their awareness.

When it comes to profiling-based decision making, even less information is provided in the privacy policies of Emotiv and NeuroSky, which do not mention the practice. However, its occurrence may be apparent based on the previous purposes for which the companies profile their users. The main aim of BCI manufacturers active in the gaming industry, like the two companies, is financial gain, attempting to increase sales as much as possible.¹⁵⁶

On the one hand, decisions based on such profiles are apparent, since the gaming experience is continuously adapted based on neurodata collected, using ML. As such, decisions of a predictive nature are continuously made by algorithms relating to what content to expose the user to in every future game played, altering parameters like the brightness of the game, and continuously improving them based on the profile created for the player, as mentioned in Appendix A para 4. Since algorithms are tasked with improving the gaming experience for the player based on the profile created about him, the natural conclusion would be that the practice falls under the scope of Article 22, solely automated decision making, including profiling. However, to qualify for protection under it, it is not enough without no human involvement, but the decisions also have to produce “legal effects concerning the data subject or similarly significantly affect the data subject”.¹⁵⁷ But because there is not enough information publicly made available by any of the companies about the calibration of the gaming experience, what it entails and its results, an analysis of solely automated decision making, including profiling under Article 22 has been decided to be outside the scope of this thesis.

On the other hand, it is not only the real-time adaptation of gaming content that facilitates achieving the monetary aim of gaming manufacturers, but also the subconscious manipulation triggered by gaming ads fed to the users.¹⁵⁸ Emotiv and NeuroSky acknowledge that they use the data collected for direct marketing purposes in Appendix A para 7 and Appendix B para 3. Companies have been known for a long time to use ad pop-ups in order to market their product,

¹⁵⁴ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (n. 22).

¹⁵⁵ See Recital 70 of the GDPR.

¹⁵⁶ B. King, (n. 62)

¹⁵⁷ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (n. 22).

¹⁵⁸ B. King, (n. 62).

attempting to influence the customer in his decisions, to their advantage.¹⁵⁹ For instance, it is a known practice that businesses use colour psychology in their advertising, as it has been scientifically proven that they are closely tied in with feelings and moods.¹⁶⁰ These strategies are most likely also employed by NeuroSky and Emotiv for direct marketing, who can adapt their ads based on the information collected through the processing of brain waves.

However, the intrinsic difference is that, through the analysis of brain waves, they can also instantly understand and predict when a customer is more inclined to buy an app due to his vulnerabilities or intentions, or even mental state and mood from that specific moment. As such, they can advertise that app at the right time to the individual, manipulating his decision, the way the display of targeted advertising in conventional gaming works, although at a much smaller scale and precision and not in real time, by virtue of personal data collected across multiple platforms. This is even more alarming when taken into consideration that the application of the other rules and safeguards enshrined in the GDPR and analysed in the second part of this chapter is less effective due to the particularities of brain data and of the technology. As illustrated, these cannot fully address profiling and profiling-based decision making in the BCI environment, and, thus, practices that are anyhow considered dangerous from a privacy and data protection perspective become extremely invasive when carried out through BCI technology by manufacturers like Emotiv and NeuroSky.

3.5. Conclusion

The peculiar characteristics of the data collected through BCI devices from the brain either potentially challenge provisions of the GDPR or render its application less effective. An impressive amount of sensitive information is inferred and used; the current data protection framework cannot fully address the special nature of brain data from the outset. This creates a loophole for commercial actors like Emotiv and NeuroSky, which do not acknowledge in fact the sensitivity of the data collected and treat it like a general category of personal data of trivial nature in practice, significantly lowering the standard of protection.

Nonetheless, even if such data is treated as general categories of personal data, fundamental concepts/principles of the utmost importance that are enshrined in the GDPR for safeguarding individuals are not properly enforced in their data processing practices, as illustrated after an assessment of the privacy policies of Emotiv and Neurosky. They are currently reporting mass revenues from their privacy infringing devices, i.e., the MWM and EE headsets. While their corporate policies try to create a data protection narrative that is compliant with the GDPR, it can be very different in terms of protection of customers' privacy and data protection rights. As such, steps need to be taken towards achieving more GDPR compliance.

4. Concluding remarks and recommendations

This paper assessed the business data processing practices of the two gaming industry leaders, Emotiv and NeuroSky, when it comes to the BCI application, and aimed at answering the question: To what extent does the GDPR offer sufficient protection to individuals subjected to

¹⁵⁹ *ibid*

¹⁶⁰ *ibid*

profiling and decision making based on profiling through electroencephalography (EEG) by the Mindwave and EPOC headsets? The thesis found that the provisions of the GDPR are either challenged, or their application is rendered less effective in this context, which leads to an insufficient level of protection for individuals subjected to these practices. This has been illustrated through an assessment of two devices based on non-invasive EEG BCI technology, the EE and MWM headsets, which operate on many occasions in blunt contrast with GDPR's data protection principles and rules.

From a technical perspective, non-invasive BCI technology presents certain special features due to the deployment of artificial stimuli and the employment of mental strategies. When combined with powerful ML algorithms like the ones embedded in the EE and MWM headsets, the devices have the potential to become a door to the mind: disseminating an extraordinary volume and variety of information. Consequently, the terms of use of NeuroSky and Emotiv do not reflect, to a large extent, the reality of the processing practices.

Much of the problem of legal incompatibility largely stems from one reason: the special nature of brain data, which either potentially challenges provisions of the GDPR or render its application less effective. Characterised by its predictive, dynamic, and uncontrollable nature, and its inherent unique link with the individual, it is considered to be a lot different from any other category of personal data. Because of these characteristics, the GDPR cannot fully address its special nature from the outset. Consequently, brain data does not qualify for special protection under the GDPR despite its differences from other general categories of personal data of trivial nature. This creates a loophole for commercial actors like Emotiv and NeuroSky, which lower the standard of protection surrounding brain data. Whilst the two companies try to create a data protection narrative that is compliant with the Regulation in their privacy policies, the reality is that their corporate practices are contrary to the law. The application of lawfulness and transparency, of the principles of purpose limitation, data minimisation, storage limitation and data security and of the rules surrounding international transfers is less effective in this context. This leads to a weaker level of protection for the users of the EE and MWM headsets when subjected to profiling and profiling-based decision making, and, in turn, to extremely invasive practices when carried out through BCI technology.

Thus, moving forward, Emotiv and NeuroSky must make extra effort to ensure that their practices are GDPR compliant. A step towards enhancing privacy, for both companies, would be embedding the BCI Anonymizer, a privacy enhancing software recommended by Bonaci et al. The software is specifically designed for BCI devices and attempts to remove any type of information other than the commands to the application from the raw EEG signals before the signals are stored.¹⁶¹ Perhaps the software can be developed to balance even better the interests of the commercial actors with those of the users. Through the ML algorithms embedded, it could be trained to separate information even better, to enable companies like Emotiv and NeuroSky to collect more information than just the commands of the users, but still not as intrusive as now. Regarding their privacy policies, Emotiv and NeuroSky could enhance transparency by letting users know about the extent of the information that can be inferred, like health data. For better explanations and more understanding of their policies, they could use a range of tools like videos, infographics, and colour coding, especially since neurotechnology is a complex topic. Additionally, since anonymisation techniques cannot be rendered fully effective for now, in this context, NeuroSky should not claim that it uses anonymisation of EEG data anymore but stick to pseudonymisation. For NeuroSky and Emotiv, these steps would be the beginning towards achieving better GDPR compliance.

¹⁶¹ T. Bonaci, R. Calo and H. Chizeck, (n. 19).

5. Appendices

Appendix A.

Emotiv's Privacy Policy

"1. Introduction

...

EMOTIV follows three guiding principles when it comes to your privacy:

- **Transparency.** We work hard to be transparent about what information we collect and process.
- **Simplicity.** We try to use easy-to-understand language to describe our privacy practices to help you make informed choices.
- **Control.** We give you control over the information you provide to us, and how it is used, shared, and retained.

...

BY (i) CLICKING "I ACCEPT EMOTIV'S PRIVACY POLICY" OR ITS EQUIVALENT OR (ii) USING OR ACCESSING THE SERVICES ON OR AFTER THE EFFECTIVE DATE IN ANY WAY, EXCEPT FOR THE SOLE PURPOSE OF REVIEWING THIS PRIVACY POLICY, YOU ARE AFFIRMATIVELY AND FREELY GIVING EMOTIV, SPECIFIC, INFORMED AND UNAMBIGUOUS INDICATION OF YOUR AGREEMENT TO THE PROCESSING OF YOUR PERSONAL INFORMATION SUBJECT TO THE TERMS OF THIS PRIVACY POLICY.

...

2. Types of Information We Collect

EMOTIV collects Personal Information about you (i) when you provide it directly to us, (ii) when third parties such as our business partners and service providers provide us with Personal Information about you, or (iii) when Personal Information about you is automatically collected in connection with your use of the Service. We collect the following Personal Information from you in connection with the Service:

Contact Information: information we collect to identify or contact you, we collect typical "business card information" such as your first and last name, physical address, email address, or telephone number. For example, this is the basic information that we collect when you register for the Service.

Financial Account Information: information that you provide in connection with your purchase of the Services (or a purchase made through the Service), including credit card number, credit card expiration date, credit card verification code, bank account number, bank account title, bank name, branch location, and routing number. You must only provide us with Financial Account Information for accounts and credit cards that you have the lawful right to access.

EEG Data: electrical biosignals collected using EMOTIV devices and any related monitoring equipment, motion sensor outputs, associated data such as event timing markers, mouse, touchscreen, gestural, and keyboard events, eye movements, survey responses, choices, and preferences, tactile, audio, visual, and other sensory stimuli, reaction times, self-assessment, and cognitive performance. It also includes information that may be inferred from the foregoing sources, either alone or in any combination.

User Account Information: information that identifies you to the Service, such as your user name, email address, password, and IP address. For example, we use this information to authenticate you when you log in to the Service, and use the IP address to help maintain your web session security while using the Service.

User Content: to the extent that you choose to input Personal Information as part of such content, images, comments, and other content, information, and materials that you post to or through the Service.

Partner Information: information that our business partners, such as our content-providing partners, share with us. For example, if you use their services to purchase, preview, and/or otherwise use their content when using the Service.

Log Data: information recorded about how you use the Services, such as IP addresses, cookies, device and browser type, geographic location, web beacons, operating system, the pages, features, products or services you browsed, the time spent viewing those pages, features, products or services, the products or services you added to your cart or purchased, the frequency with which you used the Services, search terms you used, the links on the Services that you clicked on or used, and other statistics. If you enable your browser's Do Not Track feature, EMOTIV will not be able to collect certain Log Data regarding your online activities.

Experiment Data: information collected from you during your participation in an experiment, such as your EEG Data, demographic data, performance data, and responses to experiment questions.

We sometimes collect usage and performance information that is not Personal Information. We also sometimes associate data that is not Personal Information, such as our intellectual property, with Personal Information.

3. How We Collect Personal Information

We collect Personal Information when a user (i) creates an account with EMOTIV (a "User Account"); (ii) logs into the Service; (iii) interacts with the Services (such as by submitting EEG Data); (iv) uploads or generates User Content, such as by third-party social media platforms; (v) communicates with us; (vi) responds to a communication or interaction from us; and (vii) decides to participate in an experiment.

In the event you provide EMOTIV with information about a third party, such as an employee, friend, or research or study partner, you represent and warrant to EMOTIV that you have obtained the informed written consent of such third party to: (i) provide this third-party information to EMOTIV; and (ii) allow EMOTIV to process and share this third-party information in the same manner as your information under this Privacy Policy.

4. How We Use Personal Information

We use Personal Information to: (i) provide, administer, and improve the Services; (ii) better understand your needs and interests; (iii) fulfil requests you make; (iv) personalize your experience, such as to provide you with information regarding your overall cognitive performance relative to other users of similar age or other characteristics; (v) conduct experiments you have decided to participate in; (vi) provide announcements; (vii) provide you with information and offers from EMOTIV; (viii) protect, investigate, and deter against fraudulent, harmful, unauthorized, or illegal activity; and (ix) comply with legal obligations.

5. Pseudonymization of EEG Data and Experiment Data

We use unique identifiers, such as your user ID, to process your EEG Data and Experiment Data so that it cannot be attributed to you without the use of your unique identifier. By design, we keep the unique identifier separate from your EEG Data and Experiment Data subject to technical and organizational measures to help ensure that your EEG Data and Experiment Data is not and cannot be attributed to you.

6. Lawful Basis for Processing

We will only process your Personal Information if we have a lawful basis for doing so. Lawful bases for processing include consent, contractual necessity, and our “legitimate interests” or the legitimate interest of others, as further described below.

1. **Contractual Necessity:** We process Personal Information because we need to process the data to perform our contract(s) with you, which enables us to provide you with the Service. When we process data due to contractual necessity, failure to provide such Personal Information will result in your inability to use some or all portions of the Services that require such data.
2. **Legitimate Interest:** We process some categories of Personal Information when we believe doing so furthers the legitimate interest of us or third parties. Examples of these legitimate interests include: (i) operating and improving our business, products, and services; (ii) marketing of our products and services; (iii) providing customer support; (iv) protecting from fraud or security threats; (v) complying with legal obligations; and (vi) completing corporate transactions.
3. **Consent:** In some cases, we process Personal Information based on the consent you expressly grant to us.
4. **Other Processing Grounds:** From time to time, we may also need to process Personal Information to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

7. How and With Whom We Share Information

We share Personal Information with vendors, third-party service providers, and agents who work on our behalf and provide us with services related to the Service. These parties include: (i) third parties who act for us or provide services for us, such as billing and credit card payment processing, maintenance, sales, marketing, administration, support, data enrichment, hosting, and database management services; and (ii) outside professional advisors (such as lawyers and accountants) for purposes related to the operation of our business such as auditing, compliance, and corporate governance.

We also share Personal Information when we believe it is necessary to: (i) comply with applicable law or respond to valid legal process, including from law enforcement or other

government agencies; (ii) protect us, our business or our users, or third parties, for example to enforce our terms of use, prevent spam or other unwanted communications and investigate or protect against fraud; or (iii) maintain the security of our products and services.

We share individualized and aggregated EEG Data and Experiment Data with third parties for scientific and historical research purposes.

EMOTIV may sell, transfer, or otherwise share some or all of its business or assets, including your Personal Information, in connection with a business deal (or the evaluation of a potential business deal) such as a merger, consolidation, acquisition, reorganisation, or sale of assets or in the event of bankruptcy. You acknowledge that such transfers may occur and that any acquirer or successor of EMOTIV or its assets may continue to use your Personal Information as set forth in this Privacy Policy. You may be notified via email and/or a prominent notice on the Services of any change in ownership or resulting change in uses of your Personal Information, as well as any choices you may have regarding your Personal Information.

We will not share your Personal Information with third parties without ensuring appropriate safeguards and effective and enforceable rights and remedies are in place, as required by law.

8. Security

We believe the security of your information is important and we are committed to protecting the information we receive from you. The Personal Information we collect about you is stored in limited access servers located in the United States and other countries where EMOTIV has facilities. We use commercially reasonable security measures to protect against the loss, misuse, and alteration of your information under our control based on the type of Personal Information and applicable processing activity, such as pseudonymization, data encryption in transit, and data encryption at rest.

To the extent the Services require you to provide any Financial Account Information, such as when you purchase subscriptions to the Service, that information will be collected and processed by third-party PCI-compliant service providers.

No security measures are 100% effective, however, and we cannot guarantee the security of your Personal Information. We will notify you of any data breach where your Personal Information has been obtained by unauthorized third parties, as required by law.

9. Data Retention

We retain Personal Information about you for as long as you have an open account with us or as otherwise necessary to provide you with the Service, and thereafter as set forth in any applicable agreement with you, or as set forth below. In some cases, we retain Personal Information for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule, or regulation. We retain your EEG Data for scientific or historical research purposes.

10. Third-Party Services

This Privacy Policy applies only to the Service. It does not apply to products, services, or sites that are provided by or operated by third parties, even if such products, services or sites are linked or redirected to or from the Services (“Third-Party Services”), regardless of whether or not such link or redirection is authorized by EMOTIV. Third-Party Services may have their own policies regarding privacy, or no policy at all. The fact that we link to a Third-Party Site

is not an endorsement, authorization, or representation that we are affiliated with that third party. EMOTIV is not responsible for Third-Party Services, and you use them at your own risk. We encourage you to read the privacy policies and terms of the Third-Party Services that you visit or use.

11. Your Privacy Choices

You have certain rights with respect to your Personal Information, and we want to help you review and update your information to ensure it is accurate and up-to-date.

...

Subject to certain limitations as set forth above or otherwise provided by law, you may email us at privacy@emotiv.com for any of the following:

1. **Access:** You can request more information about the Personal Information we hold about you and request a copy of such Personal Information.
2. **Rectification:** If you believe that any Personal Information we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data.
3. **Erasure:** With the exception of your EEG Data and Experiment Data, you can request that we erase some or all of your Personal Information from our systems. We retain your EEG Data and Experiment Data for scientific or historical research purposes. Please note that if you request the deletion of information required to provide the Services to you, your User Account will be de-activated and you will lose access to the Service.
4. **Portability:** You can ask for a copy of your Personal Information in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible.
5. **Withdrawal of Consent:** If we are processing your Personal Information based on your consent, you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Information, if such use or disclosure is necessary to enable you to utilize some or all of the Service. Any use of your data that has already been performed prior to our receipt of your request will not be reversed, undone, or withdrawn. If you withdraw your consent, your EEG Data and Experiment Data may still be used by us and shared with our third-party service providers to provide and improve our Services and may be shared as aggregate information that does not identify you as an individual.
6. **Objection:** You can contact us to let us know that you object to the further use or disclosure of your Personal Information for certain purposes, such as for marketing purposes.
7. **Restriction of Processing:** You can ask us to restrict further processing of your Personal Information.

...

Except as permitted by your consent to this Privacy Policy, you will be notified when your Personal Information may be shared with third parties, and you may be able to prevent the sharing of this information. To the extent permitted or required by applicable law, you can opt-out of having your information shared with a third party that is not our agent, by contacting us at privacy@emotiv.com. However, please note that opting-out of information sharing or collection may affect your ability to use some or all features of the Service.

ONCE EMOTIV PROVIDES YOUR EXPERIMENT DATA TO THE THIRD-PARTY SCIENTIST CONDUCTING THE EXPERIMENT, EMOTIV WILL BE UNABLE TO DELETE SUCH DATA FROM THE SCIENTIST'S POSSESSION.

You also have the right to lodge a complaint about EMOTIV's practices with respect to your Personal Information with the supervisory authority of your country or EU Member State.

12. Social Media Features

Some parts of the Services may include social media features. These social media features are either hosted by a third party or hosted directly on the Services. When you use these tools, the party that provides the tool, the third party that operates the social media services, and/or we may receive Personal Information about you. By using these tools, you acknowledge that some information, including Personal Information, will be transmitted to us, and that information is therefore covered by this Privacy Policy, and that some information, including Personal Information, may be shared with the third-party services, and that information is therefore governed by their privacy policies.

In general, Personal Information, once shared or disclosed, can be difficult to contain or retrieve. EMOTIV will have no responsibility or liability for any consequences that may result because you have released or shared Personal Information with others.

13. Closing Your Account

You may close an account, and upon termination of your User Account, we will take reasonable steps to provide, modify, or delete your Personal Information as soon as is practicable. However, EMOTIV may nevertheless retain your Personal Information to protect the business interests of EMOTIV, and some information may remain in archived/backup copies for our records or as otherwise required by law. Those interests include without limitation the completion of transactions, maintaining records for financial reporting purposes, complying with our legal obligations, resolving disputes, and enforcing agreements. We will retain your EEG Data for scientific or historical research purposes.

...

14. Children

The Services are not intended for children under the age of 16, and therefore, EMOTIV does not knowingly acquire or receive Personal Information from children under the age of 16. If we later learn that any user of the Services is under the age of 16, we will take appropriate steps to remove that user's information from our account database and will restrict that individual from future access to the Service. Please contact hello@emotiv.com if you are a parent or guardian of a child under 16 whom you believe has provided us with any Personal Information.

..."

Appendix B.

NeuroSky's Privacy Policy

"1. Purpose of this Privacy Policy

...

The Privacy Policy has three main purposes:

1. Explain the way we use information that you share with us in order give you a great experience with our Application;
2. Ensure that you understand what information we collect with your permission, what we do with it and with whom we share it; and
3. Explain your rights under applicable law.

All the information we collect is related to providing our Application or Service. By agreeing to our Privacy Policy, you give us the right to collect your information as detailed in this Privacy Policy and use it for the purposes described in this Privacy Policy. If you don't agree with the terms of this Privacy Policy, then please don't use the Application or Service.

2. Information we collect

The information we collect can be divided into the following broad categories:

- **Technical Data** includes internet protocol (IP) address, your login data, device type, device version, browser type and version, browser plug-ins types, time zone setting and location, traffic data, weblogs and other communications data, operating system and platform and other technology on the devices you use to access the Application.
- **Usage Data** includes information about how you use our Application or Service, such as the particular pages you interact with, how often and how long you use the Application, surveys, and the emails you interact with.
- **MindWave Data** includes the information we collect in connection with your use of MindWave. In order to operate the Application, we track your brainwave activity as recorded by MindWave. We also ask you to provide certain information regarding use of MindWave, including information related your environment and activity at the time of such use.
- **Verification Data** includes proof of identity and proof of address as further detailed in our **Subject Access Request Form**.
- **Identity Data** includes your email, date of birth, gender, username, and password, and the username and email of Authorized Account Users.

More specifically, we may collect and store the following information relating to you:

2.1 Anonymous data

When you visit our Application, we collect some basic information that does not identify individual users. This includes which pages are visited and any feedback from our visitors. We then aggregate this information with other pieces of information to improve our Application and make your experience on the Application as valuable and efficient as possible. We may also collect and accumulate anonymous data that will help us understand and analyze the online

experience of our Application users. For instance, we may accumulate visitor data relating to referring domain names, the type of browsers used, operating system software, screen resolutions, color capabilities, browser plug-ins, language settings, cookie preferences, search engine keywords and JavaScript enablement. The MindWave Data is also aggregated and used to study learning patterns.

2.2 Direct Interactions

We collect information from you when you voluntarily submit information directly to us or via our Application. For members, this refers to personal data you provide when, for example, you create an account, complete a profile, or by corresponding with us via phone, email or live chat. If you connect to the Application using credentials from a third-party application (e.g., Facebook), you authorize us to collect your authentication information, such as your username and encrypted access credentials. We may also collect other information available on or through your third-party application account, including, for example, your name, profile picture, country, hometown, email address, date of birth, gender, friends' names and profile pictures, and networks.

You may decide to provide us with another person's contact information so that person may be invited to join our Service or so that we may facilitate your communication with other people through the Service (such as when you upload an address book or a contact list). You may also provide us with another person's contact information for purposes of delivering information through social networking applications. We store the information that you provide so that the respondents may be added to your network, and also to send reminders of the invitations. All invitees are provided with the option not to receive further invitations from us.

In addition to the information we may collect upon your initial registration, we may ask you for personal information at other times. We will not share that information in a manner that identifies you as an individual with any other entity unless we have your permission.

2.3 Information submitted by you for inclusion on the Application

Information, media files and MindWave Data you may upload to the Application will be posted on the Website, subject to our [Terms of Use](#) and accessible by your Authorized Account Users; we have no control over how such visitors will use such materials. Please remember that if you post any of your personal information in study journal notes, such information may be collected and used by others over whom we have no control. We are not responsible for the use made by third parties of information you post or otherwise make available in public areas of the Application. You should take care to not use personal information in your screen name or other information that might be publicly available to other users.

2.4 Tracking technologies

We use "cookies" and similar tracking technologies (as described in **Section 5** below and in our [Cookie Policy](#)) to track your activities on our Website, and may also receive data about you if you visit other websites employing our cookies. When we send you emails that include a link to the Website, that link may contain an alphanumeric identifier that allows us to identify the person to whom we sent the message so that we can personalize our content for that individual.

2.5 Automated technologies or interactions

As you interact with our Application, we may automatically collect technical and usage data about your device, browsing actions and patterns. For example, we collect information which may include your IP address, browser type, your location, language preferences, device information and access times. While an IP address does not identify an individual by name, it may, with the cooperation of the ISP, be used to locate and identify an individual. Your IP address can reveal what geographic area you are connecting from, or which ISP you are using.

2.6 Promotions & surveys

From time to time, we may offer you the opportunity to participate in promotions such as sweepstakes, contests, offers, and/or surveys ("Special Promotions") through the Service. A Special Promotion may be governed by a privacy policy and/or terms and conditions that are additional to, or separate from, this Privacy Policy and our **Terms of Use**. If the provisions of the Special Promotion's privacy policy or terms and conditions conflict with this Privacy Policy or our **Terms of Use**, those additional or separate provisions shall prevail. If you participate in a Special Promotion, we may ask you for certain information in addition to what is stated in this Privacy Policy, including personal information. That additional information may be combined with other account information and may be used and shared as described in this Privacy Policy or in the Special Promotion.

3. How we use the information we collect

We have set out below, in a table format, a description of all the ways we process your personal data, and the legal basis we rely on to do so.

Purpose/Activity	Type of Data	Legal Basis
To allow you to use the Application	Technical Data Usage Data	Consent
To allow you to create an account	Identity Data Usage Data	Consent

To manage our relationship with you. For example general enquiries such as how the Application works, complaints and payment queries	Any data you choose to share with us or request us to view	Consent
To administer and protect the Application (including troubleshooting, fraud prevention, spam prevention, security incident prevention and correction, data analysis, testing, system maintenance, support, reporting and hosting of data), operate the Application (including notifying you of any changes), optimize your user experience, and send you service and support messages such as updates, patches and security alerts	Identity Data Technical Data Usage Data	Consent
To send you promotional messages, marketing, and other such information we think may be of interest to you, either directly or through one of our partners; you may opt out from receiving certain messages, as described in Section 7	Identity Data Technical Data Usage Data	Consent
To enable you to partake in a prize draw, competition, referral scheme, rewards program, promotional activities, events, complete a survey or invite you to participate in Application testing	Identity Data Technical Data	Consent
To analyze your use of the Application and deliver relevant Application content, for example by providing customized, personalized, or localized content, recommendations and features.	Usage Data	Consent
To enforce this Privacy Policy, our <u>Terms of Use</u> , and any other terms that you have agreed to, including to protect the rights, property, or safety of our users, or any other person.	Identity Data Usage Data Technical Data	For purposes of legitimate interests

To maintain and retain records in connection with actual and potential legal claims and regulatory investigations; and for governance & compliance purposes	Identity Data Usage Data Technical Data	Necessary for the compliance with a legal obligation to which we are subject
---	---	--

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason, and that reason is compatible with the original purpose.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

4. How we share the information we collect

When one or more of our business partners co-sponsor a service, promotion, contest/sweepstakes, or survey, we may share some or all of the information collected in connection with such service, promotion, contest/sweepstakes, or survey with the co-sponsor(s). If we intend to share such information, you will be notified prior to the collection of that information. If you do not want your information to be shared, you will be able to choose not to allow the transfer by not using or signing up for that particular service, promotion, contest/sweepstakes, or survey.

We may also share anonymized MindWave Data with educational and research institutions.

5. Cookies and other tracking technologies

A cookie is a small text file that is placed on your computer, mobile phone, or other device when you visit a website. The cookie will help website providers to recognize your device the next time you visit their website. There are other similar technologies such as pixel tags (transparent graphic images placed on a web page or in an email, which indicate that a page or email has been viewed), web bugs (similar to pixel tags), and web storage, which are used in desktop software or mobile devices.

There are also technologies such as mobile device identifiers and SDK integrations to help companies recognize your device when you return to an app or otherwise use a service.

Our policy regarding cookies can be found [here](#).

6. Information collected by third parties

Some entities that have links on our Website may collect personally identifying information about you when you access or utilize those links. We do not control the collection or use of such information, and the practices of those entities are not covered by this Privacy Policy. Links can be from content providers and/or partners who may use our logo and/or style as a result of a co-branding agreement yet they may still not follow the same policies as this Privacy Policy with respect to collection of your personal information. In addition, our Application includes social media features, such as the Facebook Like button. These features may collect

your IP address, which page you are visiting on our Application, and may set a cookie to enable the feature to function properly. Social media features and related widgets are either hosted by a third party or hosted directly on our Application. Your interactions with these features are governed by the privacy policy of the company providing them.

Please read these third parties' privacy policies to find out how they collect and process your personal information.

7. Email Opt-out

Users who no longer wish to receive email updates or other notifications may opt out of receiving these communications by following the instructions contained in the applicable email. Please know that such a decision will not stop advertising or content that is generated prior to the time when we can accomplish the removal of your information.

8. Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, altered or disclosed, used or accessed in an unauthorized way. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know it. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. However, the transmission of data via the internet is not completely secure and we cannot guarantee that unauthorized parties will not be able to defeat those measures: unauthorized entry or use, hardware or software failure, and other factors may compromise the security of our user information at any time.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

...

9. Business transitions

In the event we go through a business transition, such as a merger, acquisition by another company, or sale of a portion of our assets, users' personal information will, in most instances, be part of the assets transferred. In such instance, the new owners may use your personal data in the same way as set out in this Privacy Policy.

...

10. Users located outside of the United States

We make an effort to protect the personal information of all users of our Application. If you are unsure whether this privacy policy is in conflict with the rules applicable where you are located, you should not submit your personal information. **IN ADDITION, IF YOU ARE LOCATED WITHIN THE EUROPEAN UNION, YOU SHOULD NOTE THAT YOUR INFORMATION WILL BE TRANSFERRED TO THE UNITED STATES, THE LAWS OF WHICH MAY BE DEEMED BY THE EUROPEAN UNION TO HAVE INADEQUATE DATA PROTECTION.** Users of our Application located in countries outside of the United States who submit personal information do thereby consent to the transfer of that information to and/or storage of the information in the United States.

11. EU users' rights under the GDPR

If you are located in the European Union, or if the EU's General Data Protection Regulation ("GDPR") otherwise applies to your data as processed by us, you have the right to:

request access to your personal data. This enables you to receive a copy of the personal data we hold about you and our full list of third parties who process your data, and to check that we are lawfully processing it.

request confirmation as to whether or not your personal data is being processed.

request the correction of your personal data that you consider to be inaccurate. This enables you to have any incomplete or inaccurate data we hold about you corrected. However, we may need to verify your identity and the accuracy of the new data you provide to us.

request erasure of your personal data. This enables you to ask us to delete or remove personal data, for example: i) where there is no good reason for us continuing to process it; ii) where you have successfully exercised your right to object to processing (see below); iii) where we may have processed your information unlawfully; iv) where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons and our need to keep appropriate archives for our business operations. These reasons will be notified to you at the time of your request. In addition, as explained in Section 2.3, certain information may always be publicly available to others and other information is made publicly available to others by default.

object to processing of your personal data. This enables you to object to the processing of your personal data if you feel it impacts on your fundamental rights and freedoms. For example, this can be where we are processing your personal data for direct marketing purposes. In some cases, we may have compelling legitimate grounds to process your information which can override your right to object.

request restriction of processing of your personal data . This gives you the option to ask us to suspend the processing of your personal data in the following scenarios: i) if you want us to establish the data's accuracy; ii) where our use of the data is unlawful but you do not want us to erase it; iii) where you need us to hold the data, even if we no longer require it e.g. to establish or defend legal claims; or iv) you have objected to our use of your data but we need to verify whether we have overriding legitimate ground to use it.

request transfer of your personal data. If you request us to do so, we will provide to you, or a third party of your choice, your personal data in a commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use, or where we have used the information to perform a contract with you.

withdraw consent to the processing of your data. If you request us to do so, we will no longer process your data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent,

we may not be able to provide our Service for you. Also, we will advise you of this at the time you withdraw your consent.

not have a decision made about you based solely on **automated processing**.

...

12. Data retention

If you are located in the European Union, or if the GDPR otherwise applies to your data as processed by us, we will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or internal reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for compliance, governance, legal and/or regulatory purposes in which case we may use this information indefinitely without further notice to you.

...

13. COPPA Notice

The process described in this notice, created for children under the age of eighteen who are interested in using the Effective Learner application ("Application"), a mobile application operated by NeuroSky, Inc. ("NeuroSky") in conjunction with NeuroSky's MindWave neural headset suite of products and third-party MindWave-compatible headsets (collectively, "MindWave") and with the website located at www.effectivelearnercloud.com ("Website"), is designed to protect the privacy of your child and to comply with the Children's Online Privacy Protection Act ("COPPA"), the EU's General Data Protection Regulation ("GDPR") and related rules.

To gain access to services offered through the Application, we ask people to register with us. The registration process begins when a person electronically indicates to us his or her age. Parents, if your child indicates that he or she is under the age of eighteen, we will ask your child to provide his or her email address and your email address. Subsequently, we will email you a message asking you to confirm your birthday and your relationship with the child and instructions regarding how to set up an Effective Learner account for your child. If you opt not to activate your child's account, all information collected in the registration process will be purged from our system.

We will endeavor to ensure that only authorized employees of NeuroSky will have access to your child's personal information. Notwithstanding anything to the contrary, NeuroSky reserves the right to disclose user information when required by law, or if we have reason to believe that someone is causing injury to, or interference with, our rights or property, or the rights and property of others. In addition, in the event NeuroSky goes through a business transition, such as a merger, acquisition by another company, or sale of a portion of its assets, users' personal information will, in most instances, be part of the assets transferred. For more

information on use of information collected through the Application and Website, please view our **Privacy Policy**.

14. Disclosure of Information to Third Parties

Information generated through your child's use of the Application, including information that tracks your child's performance and progress, is accessible to third parties identified as "Authorized Account Users" through your child's account. Except for the foregoing, NeuroSky does not share its users' individually identifying information with any third parties or sponsors. Although NeuroSky may provide aggregate, statistical data to third parties, the aggregate information does not include data from which the identities of any user can be determined.

15. Parental Review of Information

Parents, if you would like to review your child's personal information, correct errors in your child's information, or delete any of your child's information, or terminate an Authorized Account User's access to your child's performance and progress records, please log onto the Website using your child's username and password. Once on the Website, proceed to your child's "Setting"-">"Profile" page. All the personal information that the App has collected from your child is listed on his or her "Profile" page. Any changes you make to the information on the "Profile" page will be effective immediately, and any electronic copies of the previous information will be automatically deleted from NeuroSky's records. If you would like to delete your child's account and/or refuse to allow any further collection or use of your child's information, please contact our Privacy Manager via email, mail or telephone. If you write to NeuroSky, please be sure to include your email address and a telephone number where we can reach you. To protect your child's privacy and security, we will take reasonable steps to verify your identity before granting you access to the personal information that we collect and maintain about your child.

...¹⁶²

6. Bibliography

Books

European Union Agency for Fundamental Rights, Council of Europe, Handbook on European data protection law, (2018)

Articles and Papers

Ahn M, Lee M, Choi J and Jun SC, 'A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users', Volume 14, Issue 8, Sensors, 2014

¹⁶² See Neurosky official website, 'Privacy policy', available at <https://effectivelearnercloud.com/el/policies/?privacy> accessed 30 May 2021.

Akhtari M, Bryant HC and Mamelak AN, 'Conductivities of three-layer human skull', Volume 14, Issue 3, Brain Topogr, 2002

Abdulkader SN, Atia A and Mostafa MS, 'Brain computer interfacing: Applications and challenges', Volume 16, Issue 2, Egyptian Informatics Journal, 2015

Arruda Leite HM, Carvalho SN, Silva Costa TB et al., 'Analysis of User Interaction with a Brain-Computer Interface Based on Steady-State Visually Evoked Potentials: Case Study of a Game', Computational Intelligence and Neuroscience, 2018

Bonaci T, Calo R and Chizeck H J, 'App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces', IEEE International Symposium on Ethics in Science, Technology and Engineering, 2014

Burwell S, Sample M and Racine E, 'Ethical aspects of brain computer interfaces: a scoping review', Volume 18, Issue 1, BMC Med Ethics, 2017

Campbell A, Choudhury T, Hu S, Lu H et al., 'Neurophone: brain mobile phone interface using a wireless EEG headset', Proceedings of the second ACM SIGCOMM workshop on Networking, Systems, and Applications for Mobile Handhelds, MobiHeld 2010, 2010

Chaudhary P and Agrawal R, 'Emerging Threats to Security and Privacy in Brain Computer Interface', Volume 3, Issue 12, Int. J. of Adv. Studies of Scientific Research, 2018

Coin A, Mulder M and Dubljev V, 'Ethical Aspects of BCI Technology: What Is the State of the Art?', Volume 5, Issue 4, Philosophies, 2020

Conti M, Mancini LV, Spolaor L and Verde NV, 'Can't you hear me knocking: Identification of user actions on android apps via traffic analysis', Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, 2015

Daly JJ and Huggins JE, 'Brain-Computer Interface: Current and Emerging Rehabilitation Applications', Volume 96, Issue 30, Arch. Phys. Med. Rehabil., 2015

Engel Jr. J, Kuhl DE, Phelps ME and Crandall PH, 'Comparative localization of epileptic foci in partial epilepsy by PCT and EEG', Volume 12, Issue 6, Annals of Neurology, 1982

Farwell LA, 'Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials', Volume 6, Issue 2, Cogn Neurodyn, 2012

Gellert R, 'Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?', Volume 16, Issue 1, Regulation and Governance, 2020

Gonzalez AR, 'EEG Signal Processing for BCI Applications', Volume 98, Issue 1, Human – Computer Systems Interaction: Backgrounds and Applications 2, 2012

Gros L, Debie N, Lete J and Leemput C, 'Video Game Addiction and Emotional States: Possible Confusion Between Pleasure and Happiness?', Front. Psychol, 2020

Hallinan D, Schutz P, Friedewald M and De Hert P, 'Neurodata and Neuroprivacy: Data Protection Outdated?', Volume 12, Issue 1, Surveillance & Society, 2014

- Huang X, Xu Y, Hua J et al., 'A Review on Signal Processing Approaches to Reduce Calibration Time in EEG-Based Brain-Computer Interface', Volume 15, Front. Neurosci, 2021
- Ienca M and Andorno R, 'Towards new human rights in the age of neuroscience and neurotechnology', Volume 13, Issue 5, Life Sciences, Society and Policy, 2017
- Jewson JJ and Thiagarajan TC, 'EEG Frequency Bands in Psychiatric Disorders: A Review of Resting State Studies', Volume 12, Issue 1, Front. Hum. Neurosc, 2019
- Kanai R, Feilden T, Firth C and Rees G, 'Political Orientations Are Correlated with Brain Structure in Young Adults', Volume 21, Issue 8, Curr Biol, 2011
- Karson CN, Coppola R, Daniel DG and Weinberger DR, 'Computerized EEG in Schizophrenia', Volume 14, Issue 193, Schizophrenia Bulletin, 1988
- Kirschstein T and Köhling R, 'What is the source of the EEG?', Volume 40, Issue 3, Clin EEG Neurosci, 2009
- Koops BJ, 'The Trouble with European Data Protection Law', Volume 4, Issue 4, International Data Privacy Law, 2014
- Krugliak A and Clarke A, 'Towards real-world neuroscience using mobile EEG and augmented reality', Volume 12, Sci. Rep, 2022
- Larsen FA, Ilyas MA, Ahmad MI and Ghani ARI, 'Classification of EEG Signals in a BrainComputer Interface System', 2016 International Conference on Robotics, Automation and Sciences (ICORAS), 2016
- Li Q, Ding D and Conti M, 'Brain-Computer Interface applications: Security and privacy challenges', IEEE Conference on Communications and Network Security (CNS), 2015
- Li M, Li F, Pan J et al., 'The MindGomoku: An Online P300 BCI Game Based on Bayesian Deep Learning', Volume 21, Issue 5, Sensors, 2021
- Liao L, Wang I, Chang C et al., 'Human Cognitive Application by Using Wearable Mobile Brain Computer Interface', TENCON 2010 - 2010 IEEE Region 10 Conference, 2010
- Liu N, Chiang C and Chin-Chu H, 'Recognizing the Degree of Human Attention Using EEG Signals from Mobile Sensors', Volume 13, Issue 8, Sensors, 2013
- Lotte F, Larrue F and Muhl C, 'Flaws in Current Human training Protocols for Spontaneous Brain-Computer Interfaces: Lessons Learned from Instructional Design', Volume 7, Frontiers in Human Neuroscience, 2013
- Martinovic I, Davies D, Frank M, Perito D, Ros T, and Song D, 'On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces', the Proceedings of the 21st USENIX Security Symposium, USENIX, 2012
- Menon V and Herbert SC, 'Combined EEG and fMRI Studies of Human Brain Function', Volume 117, Issue 3, Int Rev Neurobiol., 2005

Nicolas-Alonso LF and Gomez-Gil J, 'Brain Computer Interfaces, a Review', Volume 12, Issue 2, Sensors, 2012

Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', Volume 10, Issue 1, Law, Innovation and Technology, 2018

Rainey S, McGillivray K, Akintoye S et al., 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?', Volume 7, Issue 1, J Law Biosci, 2020

Reza FR, Allison BZ, Guger C et al., 'P300 brain computer interface: current challenges and emerging trends', Volume 5, Issue 14, Frontiers in Neuroengineering, 2012

Rui Z, Li M, Chen Q et al., 'The P300 Event-Related Potential Component and Cognitive Impairment in Epilepsy: A Systematic Review and Meta-analysis', Volume 10, Issue 1, Front Neurol, 2019

Schonberger VM, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation', Volume 17, The Columbia Science & Technology Law Review, 2016

Shih J, Krusienski D and Wolpaw J, 'Brain-Computer Interfaces in Medicine', Volume 87, Issue 3, Mayo Clinic Proceedings, 2012

Stopczynski A, Greenwood D, Hansen LK and Pentland AS, 'Privacy for Personal Neuroinformatics', Computer Science, 2014

Sullivan T.J, Deiss S.R et al., 'A Brain-Machine Interface Using Dry-Contact, Low-Noise EEG Sensors', IEEE International Symposium on Circuits and Systems, 2008

Van Erp J.B.F, Lotte F and Tangermann M, 'Brain-Computer Interfaces: Beyond Medical Applications', Volume 45, Issue 4, Computers, 2012

Van Horn JD and Toga AW, 'Human Neuroimaging as a "Big Data" Science', Volume 8, Issue 2, Brain Imaging Behav., 2014

Vecchiato G, Astolfi L, De Vico Fallani F et al., 'The study of brain activity during the observation of commercial advertising by using high resolution EEG techniques', Engineering in Medicine and Biology Society, Annual International Conference of the IEEE, 2009

Vidaurre D, Abeyesuriya R, Becker R, et al., 'Discovering dynamic brain networks from big data in rest and task', Volume 180, NeuroImage, 2018

Xu J, Yazicioglu R.F, Grundlehner B et al., 'A 160uW 8-Channel Active Electrode System for EEG Monitoring', IEEE Transactions on Biomedical Circuits and Systems, Volume 5, Issue 6, 2011

Zhang K, Xu G, Zheng X et al., 'Application of Transfer Learning in EEG Decoding Based on Brain-Computer Interfaces: A Review', Volume 20, Issue 21, Sensors, 2020

Zhang L, 'A web-based English teaching module on the administration of electroencephalography-based neurofeedback training for Chinese students', Volume 16, Issue 5, NeuroQuantology, 2018

Zhang S, Sun L, Mao X, Hu C and Liu P, 'Review on EEG-Based Authentication Technology', Volume 2021, Comput. Intell. Neurosci., 2021

Other Online Materials

Ben Wolford, 'What is GDPR, the EU's new data protection law?' (GDPR.EU), accessed via <<https://gdpr.eu/what-is-gdpr/>>

Helen Philips, 'Introduction: The Human Brain' (New Scientist, 4 September, 2006), accessed via <<https://www.newscientist.com/article/dn9969-introduction-the-human-brain/>>

Justin Banda, 'Inherently identifiable: Is it possible to anonymize health and genetic data?', (IAPP, 13 November, 2019), accessed via <<https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/>>

Kion Ahadi, 'Neurotechnology, law and the legal profession', (The Law Society, 9 August, 2022), accessed via <<https://www.lawsociety.org.uk/topics/research/how-will-brain-monitoring-technology-influence-the-practice-of-law>>

Kristof Verslype, 'Linking Together Personal Data in the Era of Big Data & GDPR' (Smals Research, 18 March, 2018), accessed via < <https://www.smalsresearch.be/data-archipelago-and-gdpr/>>

Natasha Lomas, 'Researchers spotlight the lie of 'anonymous' data', (TechCrunch, 24 July, 2019), accessed via <https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/>

Nayak CS and Anilkumar AC, 'EEG Normal Waveforms', National Centre for Biotech. Info., 2022

Reza Fazel Rezai., 'Brain-Computer Interface Systems - Recent Progress and Future Prospects', (IntechOpen, 5 June, 2013), accessed via <<https://www.intechopen.com/books/3532>>

Scott Magids, Alan Zorfas and Daniel Leemon, 'A better way to drive growth and profitability', (Harvard Business Review, November, 2015), accessed via <https://hbr.org/2015/11/the-new-science-of-customer-emotions>

The Committee on Science and Law, 'Are Your Thoughts Your Own?: Neuroprivacy and The Legal Implications of Brain Imaging', (New York City Bar, 1 June, 2005), accessed via <<https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/are-your-thoughts-your-ownneuroprivacy-and-the-legal-implications-of-brain-imagingpdf>>

Vijay Kanade, 'Top 10 Machine Learning Algorithms in 2022', (Spiceworks, 30 May, 2020), accessed via <https://www.spiceworks.com/tech/artificial-intelligence/articles/top-ml-algorithms/>>

Opinions

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, ('WP136'), 2007

Article 29WP, ‘Opinion 03/2013 on purpose limitation’, (‘WP 203’), 2013

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, (‘WP216’), 2014

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014.

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, (‘WP260’), 2017

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (‘WP251’), 2017

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, 2020

Case Law

Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016]

Websites

<https://effectivelearnercloud.com/el/policies/?privacy>

https://id.emotivcloud.com/eoidc/privacy/privacy_policy/

<https://southeast.newschannelnebraska.com/story/46355853/eeg-headset-market-2022-top-companies-report-covers-industry-outlook-in-depth-analysis-business-opportunities-and-market-share-demand-forecast-cagr>

<https://www.techtarget.com/whatis/definition/black-box-AI#:~:text=Black%20box%20AI%20is%20any,sense%2C%20is%20an%20impenetrable%20system>

<https://whatculture.com/gaming/10-manipulative-gaming-tactics-you-fall-for-every-time>